Universidade Estadual de Campinas
Instituto de Matemática, Estatística e Computação Científica
Departamento de Matemática

Rotulamentos de Códigos por Grupos de Simetrias

Marcelo Muniz Silva Alves

Orientadora **Profª. Drª Sueli Irene Rodrigues Costa**
Co – Orientador **Prof. Dr. Reginaldo Palazzo Jr.**

Tese apresentada ao **Instituto de Matemática, Estatística e Computação Científica, Unicamp**, como requisito parcial para a obtenção do título de DOUTOR EM MATEMÁTICA.

Campinas, São Paulo
Fevereiro de 2002

Rotulamentos de Códigos por Grupos de Simetrias

Este exemplar corresponde à redação final da tese devidamente corrigida e defendida por **Marcelo Muniz Silva Alves** e aprovada pela comissão julgadora.

Campinas, 07 de março de 2002

Profª. Drª Sueli Irene Rodrigues Costa
Orientadora

Prof Reginaldo Palazzo Jr.
Co-Orientador

Banca Examinadora:
Profa. Dra. Sueli Irene Rodrigues Costa
Prof. Luiz Antonio Barrera San Martin
Prof. José Plinio de Oliveira Santos
Prof. Valdemar Cardoso da Rocha Jr.
Prof. Trajano Pires da Nóbrega Neto

Tese apresentada ao **Instituto de Matemática, Estatística e Computação Científica, Unicamp**, como requisito parcial para a obtenção do título de DOUTOR EM MATEMÁTICA.

FICHA CATALOGRÁFICA ELABORADA PELA BIBLIOTECA DO IMECC DA UNICAMP

Alves, Marcelo Muniz Silva

AL87r Rotulamentos de códigos por grupos de simetrias / Marcelo Muniz Silva Alves -- Campinas, [S.P. :s.n.], 2002.

Orientador: Sueli Irene Rodrigues Costa

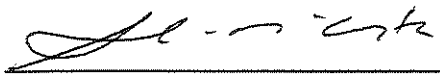
Co-orientador: Reginaldo Palazzo Júnior

Tese (doutorado) - Universidade Estadual de Campinas, Instituto de Matemática, Estatística e Computação Científica.

1. Códigos de controle de erros (Teoria da informação). 2. Grupos de simetrias. 3. Permutações (Matemática). 4. Teoria da informação. I. Costa, Sueli Irene Rodrigues. II. Palazzo Júnior, Reginaldo. III. Universidade Estadual de Campinas. Instituto de Matemática, Estatística e Computação Científica. IV. Título.

Tese de Doutorado defendida em 22 de fevereiro de 2002 e aprovada

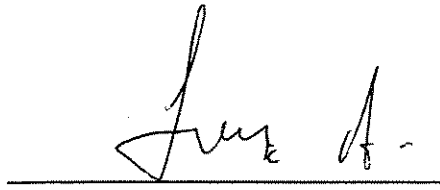
Pela Banca Examinadora composta pelos Profs. Drs.



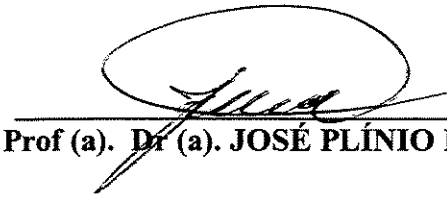
Prof (a). Dr (a). SUELI IRENE RODRIGUES COSTA

Prof (a). Dr (a). TRAJANO PIRES DA NÓBREGA NETO

Prof (a). Dr (a). VALDEMAR CARDOSO DA ROCHA JR.



Prof (a). Dr (a). LUIZ ANTONIO BARRERA SAN MARTIN



Prof (a). Dr (a). JOSÉ PLÍNIO DE OLIVEIRA SANTOS

Resumo

A tese versa sobre questões relativas a grupos de simetrias de códigos e sua utilização no rotulamento destes códigos. Um código é rotulável por um grupo G se este grupo age como grupo de simetrias de modo livre e transitivo; os rotulamentos são as bijeções naturais entre o grupo e suas órbitas. A importância disto vem das isometrias associadas entre anéis e códigos que vêm sendo usadas para obtenção de novos exemplos a partir de construções já conhecidas. Neste trabalho utilizamos grupos de simetrias de códigos em dois problemas distintos: o primeiro, sobre extensões de códigos quaternários via isometrias entre anéis e códigos em espaços de Hamming, e o segundo sobre códigos em grafos que incluem os espaços de Lee. Um dado interessante é que todos os grupos envolvidos podem ser escritos como produto semi-direto de dois grupos simétricos ou de um grupo simétrico por um grupo abeliano (mais especificamente, o produto é o "wreath product" destes grupos).

Na parte relativa a espaços de Hamming, os resultados principais são a descrição dos códigos propelineares como órbitas de grupos de simetrias e suas relações com os códigos G-lineares; a demonstração da inexistência de rotulamentos cíclicos de espaços de Hamming em geral; a determinação dos grupos de simetrias dos códigos de Reed-Muller generalizados de primeira ordem e rotulamentos cíclicos para estes códigos. A existência destes rotulamentos é conhecida de trabalhos anteriores, e aqui fornecemos uma descrição alternativa, a qual determina todos os rotulamentos no caso binário. Além disso, mostramos que as simetrias que rotulam RM(1,m) não se estendem a isometrias do espaço ambiente.

Quanto aos códigos sobre grafos, os principais resultados são a explicitação de relações entre códigos em grafos e ladrilhamentos do espaço euclidiano; a construção de um grupo rotulador não-abeliano para uma família de espaços de Lee; e a descrição de todos os códigos perfeitos de Lee em dimensão 2, via a consideração do problema de ladrilhamentos associado (estendendo resultados clássicos sobre estes códigos).

Abstract

This work deals with questions related to symmetry groups of codes and their use as code labelings. A code is labeled by a group G if this group acts freely and transitively as a group of symmetries; the labelings are the natural bijections between the group and its orbits. The importance of labelings comes from the associated isometries between rings and codes which have been used as a means of constructing new codes from old ones. In this work we use symmetry groups of codes in two different problems: the first one, on extensions of quaternary codes via isometries between rings and codes in Hamming spaces, and the second on codes in graphs that include Lee spaces. An interesting feature is that all the groups involved can be expressed as wreath products of two symmetric groups or of a symmmetric group and an abelian group.

Concerning Hamming spaces, the main results are the description of propelinear codes as orbits of symmetry groups and the determination of its relationship with G-linear codes; the proof of the non-existence of cyclic labelings of general Hamming spaces; the determination of the symmetry groups of the generalized first-order Reed-Muller codes and of cyclic labelings for these codes. The existence of these labelings is known from previous works, but here we provide an alternative description that determines all the labelings in the binary case. In addition, we show that the symmetries that label $RM\,(1, m)$ are not extendable to symmetries of the ambient space.

With respect to codes on graphs, the main results are the establishment of the relations between codes on graphs and tesselations of euclidean space; the construction of a non-abelian labeling group for a family of Lee spaces; and the description of all linear perfect Lee codes in dimension two, via the associated tesselation (thus extending classical results on these codes).

Notação

F_q denota o corpo finito de q elementos (único, a menos de isomorfismos).
$\mathbb{S}(M,d)$ é o grupo de simetrias do espaço métrico (M,d).
$\mathbb{S}(C)$ é o grupo de simetrias do código $C \subset (A^n,d)$, ou seja, o grupo de simetrias do espaço métrico $(C,d|_C)$.
$\mathbb{S}(C,A^n)$ é o grupo das simetrias de (A^n,d) que preserva o código C (se $f \in \mathbb{S}(C,A^n)$ e $u \in C$, então $f(u) \in C$).
S_n é o grupo simétrico de grau n, ou seja, o grupo de todas as permutações de um conjunto de n elementos.
$\mathbb{Z}_m$ será usado tanto para o anel modular $\mathbb{Z}/m\mathbb{Z}$ quanto para o grupo cíclico de m elementos (que é o grupo aditivo de anel $\mathbb{Z}/m\mathbb{Z}$). Nas passagens em que estivermos tratando de ambos, como quando estivermos falando tanto do anel quanto do grupo cíclico, denotaremos este último por $(\mathbb{Z}_m,+)$.
$H \rtimes G$ indica um produto semi-direto de G por H, onde H age em G. Neste texto, este produto será quase sempre um "wreath product".
$GRM(1,k)_q$ é o código de Reed-Muller (generalizado) de primeira ordem sobre o corpo F_q.
$RM(1,k)$ é o código de Reed-Muller binário.

Agradecimentos

Em primeiro lugar, agradeço à Professora Sueli Costa pela dedicação e apoio durante o trabalho, e por seu espírito de iniciativa durante todo este tempo. Os resultados obtidos aqui devem muito ao esforço e incentivo da orientadora.

Agradeço também ao Professor Reginaldo Palazzo Jr., por seu convite à nossa participação nesta pesquisa multidisciplinar, e por sua dedicação e trabalho desde então.

Agradeço à Fapesp, pela bolsa que permitiu a realização deste trabalho, bem como pelo apoio técnico e financeiro durante o doutorado.

Agradeço aos Professores Edson Agustini, João R. Gerônimo e Martinho Araújo pelo frutífero trabalho em conjunto.

Agradeço aos Professores Luiz San Martin e Marcelo Firer, pela realização de vários seminários em conjunto e pelas idéias e sugestões dadas nestes seminários e em outras ocasiões.

Agradeço ao Professor Thomas Honold, pela generosidade em nos indicar trabalhos importantes na área, e em nos facilitar o acesso a estes trabalhos.

Agradecimentos são devidos a um revisor anônimo, cujas críticas a um artigo nosso deram origem à pesquisa que constitui o último capítulo desta tese.

Também agradeço a toda a minha família, em especial a meus pais. Não teria chegado até aqui se não fosse por eles.

Um agradecimento especial: à Sílvia, por estes anos juntos, pelas idéias brilhantes, pela alegria, por muitas coisas mais. Mesmo que teime em não aceitar que infinito mais um não é maior que infinito.

Introdução

Rotulamentos

Rotulamentos, ou parametrizações, de códigos são um instrumental comum em se tratando do estudo de códigos esféricos de espaços euclidianos, onde se consideram grupos discretos de transformações ortogonais. De modo geral, diremos que o código C é rotulado pelo grupo de simetrias G se este grupo age livre e transitivamente em C. A utilização de grupos rotuladores na construção de exemplos em espaços métricos discretos ainda é restrita, talvez porque leve naturalmente a códigos não-lineares, onde há menos ferramentas disponíveis do que no caso linear. Por outro lado, rotulamentos são um meio de compensar a não-linearidade, fornecendo uma estrutura algébrica a códigos não-lineares. E são também um meio de obter bons códigos sobre corpos a partir de outros sobre anéis, através de rotulamentos de códigos clássicos, como alguns códigos MDS e os códigos de Reed-Muller de primeira ordem.

As aplicações de rotulamentos ao estudo de códigos em espaços discretos têm sua maior motivação nos códigos quaternários. Estes códigos, também chamados de $\mathbb{Z}_4$-lineares, são obtidos via uma isometria entre o espaço de Lee $(\mathbb{Z}_4^n, d_l)$ e o espaço de Hamming $\left(\mathbb{Z}_2^{2n}, d_h\right)$. O primeiro código a ser reconhecido como quaternário foi o de Kerdock, o que foi feito em [32]. Mas o trabalho que realmente inaugurou esta área é o artigo [22], em que questões pendentes até então são resolvidas via a associação entre códigos sobre $\mathbb{Z}_2^{2n}$ e códigos lineares sobre $\mathbb{Z}_4^n$.

Um segundo exemplo importante de aplicação de rotulamentos ao estudo de códigos é o dos códigos propelineares. Estes códigos foram definidos em [37] como um modo de descrever códigos binários perfeitos, um programa que é realizado em [6]. A cada código propelinear é associado um grupo de permutações de coordenadas satisfazendo algumas condições, de modo a definir uma estrutura de grupo sobre o código.

Uma terceira construção, a G-linearidade, feita de modo a estender o conceito da $\mathbb{Z}_4$-linearidade, utiliza diretamente os grupos de simetrias do espaço ambiente. Na G-linearidade buscam-se grupos de simetrias que parametrizem o espaço todo, ou seja, que tenham uma ação livre e transitiva no espaço ambiente. Os códigos então correspondem a órbitas de subgrupos de G. Para famílias de espaços métricos (M^n, d), como os de Hamming e de Lee, pode-se estender a ação de G coordenada a coordenada, e deste modo obter uma ação de G^k em $\left(M^{kn}, d\right)$. Assim consideram-se também subgrupos de G^n e suas órbitas, de modo análogo ao que é feito na $\mathbb{Z}_4$-linearidade.

Outra aplicação é relacionada à conexão entre códigos e reticulados. Esta conexão vem sendo explorada há tempos para a construção de reticulados a partir de códigos: um bom exemplo é a construção A de Sloane, que consiste usar a projeção canônica $p : \mathbb{Z}^n \to \mathbb{Z}_2^n$ para definir reticulados em $\mathbb{R}^n$ como pré-imagens de códigos binários[11]. Pode-se também usar o caminho inverso, como é feito em [20] na construção de códigos de Lee perfeitos.

O ponto em comum entre todas estas construções é que são ou diretamente definidas por rotulamentos, ou existe uma construção mais intrínseca e equivalente por rotulamentos.

$\mathbb{Z}_4$-linearidade, G-linearidade, Propelinearidade e Rotulamentos

O conceito de código $\mathbb{Z}_4$-linear deu origem a um fértil campo de pesquisa tanto em códigos binários como em construção de reticulados em $\mathbb{R}^n$. Naturalmente buscaram-se extensões disto que permitissem o uso das mesmas técnicas, o que levou à consideração de pesos (métricas invariantes) sobre R-módulos e isometrias entre estes módulos e códigos. Mesmo nesta generalidade, é fácil verificar que um R-módulo M dotado de uma métrica invariante d é isométrico a um espaço métrico (C, d') se e só se o grupo aditivo $(M, +)$ age (livre e transitivamente) como grupo de simetrias em C (Capítulo 1, Seção 1.3, Lema 1). Em particular, os códigos quaternários correspondem a códigos binários invariantes sob a ação de um grupo de rotações isomorfo a $(\mathbb{Z}_4^n, +)$. Isto é discutido com mais detalhes no Capítulo 1.

Assim, o estudo dos rotulamentos abelianos de um código é equivalente ao estudo de isometrias entre módulos e este código, e extensões da $\mathbb{Z}_4$-linearidade para uma $\mathbb{Z}_m$-linearidade correspondem a rotulamentos cíclicos de códigos. Sobre esta questão temos algumas respostas parciais. A versão G-linear desta extensão, por exemplo, requereria um rotulamento cíclico do espaço ambiente. Este problema foi considerado em [13] para espaços de Lee, onde mostramos que o único rotulamento é o de $\mathbb{Z}_2^2$ por $\mathbb{Z}_4$ (ver também [19, 30, 28]). O mesmo problema foi considerado em [39] para isometrias entre $\mathbb{Z}_{p^k}$ e o espaço de Hamming $\left(\mathbb{Z}_p^k, d_h\right)$, p primo. A resposta também é negativa. Esta conclusão vale para todos os espaços de Hamming distintos de $\left(\mathbb{Z}_2^2, d_h\right)$, como mostraremos no Capítulo 4 (Seção 4.2 ,Teorema 16).

As extensões existentes são, portanto, para rotulamentos de códigos e não do espaço total. Rotulamentos cíclicos de códigos em espaços de Hamming são o tema do Capítulo 4.

No caso binário, as isometrias efetivamente usadas são feitas com o anel $\mathbb{Z}_{2^k}$. Há vários motivos para a restrição a um alfabeto de 2^k elementos. Entre outras coisas, isto permite uma comparação mais direta com códigos binários lineares – que sempre possuem 2^m elementos – e também o uso de técnicas como o levantamento de Hensel. Este é um método de obter códigos em $\mathbb{Z}_{2^k}^n$ a partir de outros pré-existentes sobre $\mathbb{Z}_2^n$, e foi utilizado em [22] no âmbito de códigos $\mathbb{Z}_4$-lineares. Nestas condições temos os códigos $\mathbb{Z}_{2^k}$-lineares de [9], que são construídos a partir de uma isometria entre um espaço métrico sobre $\mathbb{Z}_{2^{k+1}}$ e o código de Reed-Muller de primeira ordem $RM(1, k)$. Aqui nós reconstruiremos esta isometria a partir de rotulamentos do código biortogonal, que é o código esférico obtido ao se trocar 1 por -1 e 0 por 1 nas palavras de $RM(1, k)$ (Capítulo 4, seção 4.3.4).

A isometria binária foi estendida a uma isometria entre uma classe de anéis finitos e os códigos

$GRM\,(1,k)_q$, os códigos de Reed-Muller de primeira ordem sobre um corpo finito F_q em [21]. Como consequência, existem isometrias entre anéis $\mathbb{Z}_{p^k}$ e estes códigos. Vários códigos de bons parâmetros – binários e ternários – foram obtidos via o levantamento de Hensel composto com estas aplicações [9, 17, 21]. Para construí-las explicitamente como rotulamentos, nós calculamos o grupo de simetrias dos códigos $GRM\,(1,k)_q$ (Capítulo 4, Seção 4.3). O mesmo método é utilizado para construir rotulamentos por $\mathbb{Z}_{q^2}$ do código de Reed-Solomon sobre F_q, estendendo uma isometria apresentada em [16] (Capítulo 4, Seção 4.3.2).

Os códigos propelineares, por sua vez, também correspondem a rotulamentos por grupos de simetrias. O caminho para chegar a este resultado é mais longo, e esta "tradução" é o tema do Capítulo 3. Nesta parte do trabalho nós mostramos como chegar aos propelineares via rotulamentos e estabelecemos as relações existentes entre estes códigos e códigos G-lineares binários (Capítulo 3, Seção 3.2, Teorema 11, e também Seção 3.3). A associação entre códigos binários e esféricos que usamos para os códigos de Reed-Muller também aparece aqui, de modo essencial, na construção de novos exemplos de códigos propelineares e G-lineares (Capítulo 3, Seções 3.2 e 3.3). Particularmente, há um novo exemplo de códigos propelineares feito a partir de álgebras de Clifford (Capítulo 3, Seção 3.2, Exemplo 8).

Devemos chamar a atenção para o fato de que vários dos rotulamentos cíclicos do Capítulo 4, envolvendo códigos de Reed-Muller e de Reed-Solomon, não se encaixam em nenhum destes dois conceitos: não são nem G-lineares, nem propelineares. No caso do Reed-Muller binário, podemos afirmar com certeza que nenhum rotulamento é feito por uma isometria que venha do espaço ambiente. Ou seja, as isometrias cíclicas são isometrias do espaço métrico $(RM\,(1,k)\,,d_h)$ que não vêm de isometrias de $\left(\mathbb{Z}_2^{2^k},d_h\right)$ (Capítulo 4, Seção 4.3.4, Teorema 22). Elas não se estendem ao espaço ambiente. Não há certeza quanto aos outros casos, mas o código de Reed-Solomon possui simetrias inextensíveis, e é provável que os outros códigos de Reed-Muller também as possuam. Estas questões são tratadas no Capítulo 4, onde também fornecemos estimativas parciais para a menor dimensão possível em que se encontra um código com rotulamento cíclico (Capítulo 4, Seção 4.3.2, Teorema 21).

Rotulamentos de espaços de Lee e códigos perfeitos em dimensão 2

Códigos perfeitos em espaços de Lee e rotulamentos destes espaços são estudados no Capítulo 2. Para estas questões é vantajoso trabalhar com espaços de Lee como quocientes de grafos. O grafo original é o grafo canônico sobre $\mathbb{Z}^n$, em que dois vetores u,v são ligados se e só se $u-v=\pm e_i$. A projeção $\mathbb{Z}^n\to\mathbb{Z}_m^n$ induz uma estrutura de grafo em $\mathbb{Z}_m^n$ que define a métrica de Lee. Esta construção, mais o fato de que todas as simetrias de $(\mathbb{Z}_m^n,d_l)$ são induzidas de isometrias euclidianas, pemite relacionar códigos de Lee e ladrilhamentos de $\mathbb{R}^n$. No capítulo 2 vamos estabelecer correspondências entre ladrilhamentos de $\mathbb{R}^n$, ladrilhamentos de toros e códigos em espaços de Lee.

A primeira aplicação é em códigos lineares perfeitos bidimensionais. Nós fornecemos uma descrição completa destes códigos, mostrando que para cada número natural m da forma $m = k\left(2n^2 + 2n + 1\right)$ existem exatamente dois destes códigos em $\left(\mathbb{Z}_m^2, d_l\right)$. Também verificamos que ambos são equivalentes, isto é, que existe uma isometria linear que leva um em outro. Isto é feito via o estudo do problema associado de ladrilhamento do plano (Capítulo 2, Seção 2.4, Teoremas 8 e 9).

A segunda aplicação é na construção de um rotulamento do espaço total, que sabemos ser ou dado pelo grupo de translações, ou por um grupo parametrizador não-comutativo [30, 28]. Este caso também é resolvido por meio da construção de um ladrilhamento em $\mathbb{R}^n$. A parametrização feita é então quocientada para toros onde se realizam os espaços de Lee. Este rotulamento é um exemplo de G-linearidade, onde G é o grupo rotulador, que é isomorfo a $\mathbb{Z}_m^n \rtimes \mathbb{Z}_2^n$ (Capítulo 2, Seção 2.5).

Sumário

Capítulo 1

Fundamentos

Neste capítulo reunimos os conceitos fundamentais de teoria de códigos necessários para este trabalho. As fontes são MacWilliams/Sloane [27], Conway/Sloane [11] e Tsfasman/Vladut [41]. Algumas definições não são exatamente as mesmas, mas são sempre generalizações naturais das originais.

As descrições dos grupos de simetrias dos espaços de Hamming e de Lee são indispensáveis no que se segue, e por isso também estão presentes neste capítulo. Estudamos com detalhes o caso de espaços de Lee em [13, 30, 28]. Uma demonstração do caso de Hamming pode ser vista em [15].

1.1 Conceitos Fundamentais

Definição 1 *Seja (M, d) um espaço métrico. Um código é um subconjunto discreto de M.*

Esta noção mais geral de código remete a [15]. Há pelo menos dois casos bem distintos aqui: M contínuo e M discreto (e neste caso M é finito, em geral). No primeiro caso, M costuma ser o espaço euclidiano $\mathbb{R}^n$, a esfera S^n, ou (mais raramente) os espaços projetivos $\mathbb{RP}^n$ e $\mathbb{CP}^n$. Como já foi mencionado, os códigos em esferas costumam estar associados a grupos de transformações ortogononais, e os códigos em $\mathbb{R}^n$ costumam estar associados a reticulados. Existe uma associação simples entre códigos esféricos e códigos binários (códigos em $\mathbb{Z}_2^n$), a aplicação $\eta(a_1, \ldots, a_n) = ((-1)^{a_1}, \ldots, (-1)^{a_n})$. Ela será utilizada como um meio de obter exemplos em espaços discretos via grupos ortogonais.

Em espaços finitos temos duas métricas clássicas: as métricas de Hamming e de Lee, que são as que nos ocuparão neste trabalho. Em ambos os casos o espaço M é do tipo A^n, onde A é chamado de alfabeto do código. Para a de Hamming pode-se usar qualquer alfabeto A, mas em geral A tem ao menos a estrutura de grupo abeliano. Por sua vez, a métrica de Lee é definida apenas sobre produtos cartesianos de $\mathbb{Z}_m$. Códigos sobre espaços do tipo (A^n, d), onde a métrica d vem de uma métrica d' sobre A, costumam ser chamados de códigos de bloco.

Seja então A um conjunto não-vazio. O espaço de Hamming (A^n, d_h) tem a seguinte função distância: dados $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n) \in A^n$,

$$d_h\left((u_1, \ldots, u_n), (v_1, \ldots, v_n)\right) = \sum_{i=1}^{n} \delta(u_i, v_i),$$

onde $\delta(a, b) = 0$ se $a = b$, e $\delta(a, b) = 1$ se $a \neq b$.

Os espaços de Lee são definidos apenas sobre os $\mathbb{Z}_m$-módulos $\mathbb{Z}_m^n$. Os unidimensionais são isométricos a espaços de m pontos uniformemente distribuídos sobre um círculo. Em $\mathbb{Z}_m^n$, a métrica de Lee é definida pela soma das distâncias entre as coordenadas: dados $u = (u_1, \ldots, u_n)$ e $v = (v_1, \ldots, v_n) \in \mathbb{Z}_m^n$,

$$d_l\left((u_1, \ldots, u_n), (v_1, \ldots, v_n)\right) = \sum_{i=1}^{n} \min\left\{|u_i - v_i|, m - |u_i - v_i|\right\}.$$

Nota-se claramente que a métrica de Lee é invariante: $d(u, v) = d(u - v, 0)$. O mesmo ocorre com o espaço de Hamming (A^n, d_h) quando A tem estrutura de grupo abeliano. Deste modo, a métrica é determinada pela função $w(u) = d(u, 0)$. Esta função é chamada *peso* de u. Em geral, estas funções são definidas sobre espaços vetoriais e módulos.

Definição 2 *Seja R um anel, M um R-módulo. Uma função $w : M \to \mathbb{R}$ é uma função peso se a aplicação $d(u, v) = w(u - v)$ é uma métrica sobre M.*

Este conceito aparece em, por exemplo, isometrias entre anéis de cadeia finitos e códigos de Reed-Muller de primeira ordem [21]. Voltaremos a isso quando estivermos tratando de rotulamentos de códigos.

As comparações entre códigos são feitas com base em alguns parâmetros básicos. Dentre estes se destacam a distância mínima, o número de pontos do código, e o seu comprimento.

Definição 3 *A distância mínima de um código C é o número $d = \min\{d(x, y) | x, y \in C, x \neq y\}$. O comprimento de um código C em (A^n, d) é a dimensão do espaço ambiente, n.*

Deste modo, d mede o "espalhamento" dos pontos de C. O problema fundamental em teoria de códigos é dado em termos destes parâmetros: no espaço (M, d), procuramos códigos com a maior distância mínima e maior número de pontos possíveis. Logicamente, estes são objetivos conflitantes: uma melhor maneira de tratar este problema é fixar alguns parâmetros. Por exemplo, dados k e n, procurar o código com a maior distância mínima possível. Outro problema: fixados n e d, encontrar códigos com o maior k possível e com distância mínima maior do que (ou igual a) d.

A distância mínima diz respeito à capacidade de correção do código. Nós dizemos que um código C é capaz de corrigir t erros se as bolas de raio t centradas em pontos de C têm intersecção vazia; isto vem da interpretação dos pesos de vetores como erros em transmissões por canais gaussianos. Neste modelo, um vetor v_0 é transmitido, e um vetor $v_0 + e$ é recebido, onde a

probabilidade de que o peso de e seja r decresce exponencialmente com r. A codificação é um modo de corrigir os erros cometidos na transmissão: os vetores transmitidos são os elementos do código (também chamados palavras do código). Deste modo, se o vetor recebido na transmissão é u, e u pertence à bola $B_t(v)$, onde v pertence ao código, decidimos que o vetor transmitido foi v. Esta é a chamada decodificação pelo vizinho mais próximo (nearest neighbor decoding). O vetor erro, neste caso, é o vetor $e = u - v$, que tem peso menor do que t. Logo, se a probabilidade de ocorrer mais do que t erros na transmissão é desprezível, esta decodificação recupera o vetor correto quase sempre. Uma exposição mais detalhada do modelo gaussiano e das aplicações de códigos em Teoria da Informação pode ser encontrada em [1] e [27].

A relação da distância mínima com a capacidade de correção é direta: se o código C possui distância mínima d, então duas bolas de raio $t = \lfloor (d-1)/2 \rfloor$ centradas em pontos distintos de C não se interceptam, e o código pode corrigir até t erros, e não mais que isso. O número t também é chamado de raio de empacotamento do código[1].

Quanto à estrutura, podemos afirmar sem exagero que quase todos os códigos conhecidos são lineares.

Definição 4 *Seja (A^n, d) um espaço métrico, onde A, o alfabeto, é um anel. Então um código C de (A^n, d) é dito linear se é um submódulo livre de A^n. Para códigos lineares sobre o corpo F_q de cardinalidade q é usada a notação $[n, k, d]_q$, sendo k a dimensão do código (como subespaço vetorial).*

Os códigos lineares são muito importantes por várias razões. Em geral, quanto mais estrutura o código possui, mais ferramentas existem para o cálculo da distância mínima e de sua cardinalidade. Além disso, passos importantes na implementação e na decodificação dependem da linearidade. Por outro lado, há uma limitação nas possibilidades de número de pontos e distância mínima, e é aqui que reside o interesse em códigos não-lineares. Alguns dos melhores códigos conhecidos são não-lineares, e foi a pesquisa sobre alguns destes códigos, como os códigos de Kerdock, que levou ao conceito de código quaternário.

O código linear $\mathcal{C}$ pode ser sucintamente descrito pela notação $[n, k, d]$, que lista seus parâmetros fundamentais. Também se usa esta notação para códigos não-lineares, sendo que neste caso $k = \log_{|A|} |\mathcal{C}|$ (também se encontra a notação $(n, |\mathcal{C}|, d)$ para códigos não-lineares e códigos esféricos). Uma informação mais completa sobre o perfil de distâncias do código linear $\mathcal{C}$ é dada pelo polinômio enumerador de $\mathcal{C}$, definido a seguir.

Definição 5 *Seja $\mathcal{C}$ um código em (A^n, d), A um anel, w o peso associado a d. O polinômio enumerador de $\mathcal{C}$ é $w_{\mathcal{C}}(t) = \sum_{u \in \mathcal{C}} t^{w(u)}$.*

[1] Esta é a definição para espaços métricos discretos.No caso geral, o raio de empacotamento é o supremo dos números s tais que duas bolas quaisquer de raio s tem intersecção nula.

Em outras palavras, $w_{\mathcal{C}}(t) = \sum_{i=0}^{m} a_i t^i = 1 + a_d t^d + \ldots + a_m t^m$, onde o coeficiente a_i de t^i é igual ao número de elementos de $\mathcal{C}$ cujo peso é igual a i. Este polinômio também pode ser usado para códigos não-lineares que contém a origem e que são homogêneos - isto é, que possuem grupo de simetrias transitivo. Em espaços de Hamming, outro polinômio usado para códigos lineares é o polinômio homogêneo $\widetilde{w}_{\mathcal{C}}(x,y) = \sum_{u \in \mathcal{C}} x^{w(u)} y^{n-w(u)}$, n o comprimento do código. Note que $w_{\mathcal{C}}(t) = \widetilde{w}_{\mathcal{C}}(t,1)$.

Finalmente, mencionamos uma classe importante de códigos que irá aparecer no trabalho: a dos códigos perfeitos. Em geral, se o código corrige t erros, a união das bolas $B_t(v)$ não cobre o espaço inteiro. Nós chamamos de raio de cobertura do código o menor inteiro r tal que $A^n = \bigcup_{v \in \mathcal{C}} B_r(v)$. Logicamente, temos $t \leq r$ em qualquer espaço métrico. Quando ocorre a igualdade, temos um código perfeito.

Definição 6 *Um código $\mathcal{C}$ é* perfeito *quando os raios de empacotamento e de cobertura são iguais.*

Em espaços de Hamming são conhecidos todos os códigos perfeitos lineares. Em espaços de Lee existem apenas resultados parciais, e neste texto daremos uma contribuição no caso bidimensional.

1.2 Simetrias e Automorfismos

Em Teoria de Códigos, as questões são usualmente de natureza geométrica (como a busca do melhor código possível com parâmetros k e n fixados) ou motivadas por considerações geométricas (como o problema de encontrar algoritmos de decodificação que sejam boas aproximações da decodificação por probabilidade máxima). Deste modo, é de se esperar que as transformações naturais sejam isometrias, que são agrupadas em três classes: isometrias do código que se estendem ao espaço ambiente, isometrias inextensíveis, e isometrias lineares, chamadas de automorfismos.

O estudo dos automorfismos é motivado pela classe dos códigos lineares, pois estas são as isometrias que preservam esta classe. Começamos pelo grupo de automorfismos dos espaços de Hamming.

Definição 7 *Seja F_q um corpo finito. O grupo monomial sobre F_q^n consiste das matrizes quadradas de ordem n cujos vetores coluna possuem exatamente uma entrada não-nula.*

Este grupo é o grupo de isometrias lineares de $\left(F_q^n, d_h\right)$, e pode-se ver facilmente que é isomorfo a $\left(F_q^*\right)^n \rtimes S_n$ (onde F_q^* é o grupo multiplicativo $(F_q - \{0\}, \cdot)$). Dois códigos lineares são ditos equivalentes se são associados por uma matriz monomial. As transformações monomiais que fixam um código $\mathcal{C}$ formam o seu grupo de automorfismos, denotado por $Aut(\mathcal{C})$.

No caso de espaços de Lee, o grupo de isometrias lineares coincide com o grupo de isometrias que fixam a origem. Este grupo é isomorfo ao grupo de matrizes ortogonais reais cujas colunas possuem uma entrada igual a 1 ou -1, e todas as outras nulas [13]. O grupo pode ser descrito como $\mathbb{Z}_2^n \times S_n$.

Ao considerar também códigos não-lineares somos levados a incluir todas as simetrias possíveis, e não só as lineares. Os grupos de simetrias dos espaços de Hamming e de Lee são conhecidos:

Teorema 1 *1. [15] Seja (A^n, d_h) o espaço de Hamming sobre A^n, onde A tem m elementos. O grupo $\mathbb{S}(A^n, d_h)$, o grupo de simetrias de (A^n, d_h), é isomorfo ao grupo $S_m^n \times S_n$.*

2. [13] O grupo de simetrias do espaço de Lee $(\mathbb{Z}_m^n, d_l)$ é isomorfo ao grupo $\mathbb{Z}_m^n \times (\mathbb{Z}_2^n \times S_n)$.

Para uma melhor compreensão da ação destes grupos, vamos descrever como agem os fatores de cada um. No caso de (A^n, d_h), seja $u = (u_1, \ldots, u_n) \in A^n$ e $\pi \in S_n$. Então

$$\pi u = \left(u_{\pi^{-1}(1)}, \ldots, u_{\pi^{-1}(n)}\right),$$

isto é, S_n age por permutação de coordenadas. O grupo S_m^n age coordenada a coordenada: dado $\sigma = (\sigma_1, \ldots, \sigma_n) \in S_m^n$,

$$\sigma u = (\sigma_1 u_1, \ldots, \sigma_n u_n).$$

Toda isometria se fatora como produto de uma permutação de coordenadas por um elemento de S_m^n. O grupo também pode ser descrito como um grupo de matrizes. A representação (real) pode ser feita do seguinte modo: tomamos o espaço vetorial gerado pelo conjunto $\beta = \{e_{ij}; i = 1, 2, \ldots, n \text{ e } j \in A\}$. Nesta base, a ação é descrita por $(\sigma, \pi)(e_{ij}) = e_{\pi(i)\sigma_{\pi(i)}j}$. A representação é definida pela extensão linear desta ação. Deste modo, pode-se identificar o ponto $(a_1, \ldots, a_n)$ com o vetor $e_{1a_1} + \ldots + e_{na_n}$ e considerar a ação de $S_m^n \times S_n$ no conjunto $\widetilde{A}^n = \{e_{1a_1} + \ldots + e_{na_n}; a_i \in A\}$ como uma ação equivalente à de $S_m^n \times S_n$ como grupo de simetrias do espaço de Hamming (A^n, d)[2].

Nos espaços de Lee é mais fácil dar uma representação matricial sobre o próprio alfabeto $\mathbb{Z}_m$. O grupo de isometrias lineares é isomorfo a $\mathbb{Z}_2^n \times S_n$. Como no caso anterior, S_n age permutando coordenadas, e $\mathbb{Z}_2^n$ age como S_m^n. O grupo $\mathbb{Z}_m^n$ corresponde às translações de $(\mathbb{Z}_m^n, d_l)$. Uma representação deste grupo (sobre $\mathbb{Z}_m$) é dada pelo grupo de matrizes

$$M = \begin{bmatrix} a_{11} & \ldots & a_{1n} & v_1 \\ \vdots & & \vdots & \vdots \\ a_{n1} & \ldots & a_{nn} & v_n \\ 0 & \ldots & 0 & 1 \end{bmatrix}$$

onde (a_{ij}) é monomial com entradas não-nulas ± 1, e $v_i \in \mathbb{Z}_m$. Identificando $\mathbb{Z}_m^n$ com o hiperplano $\mathbb{Z}_m^n \times \{1\} \subset \mathbb{Z}_m^{n+1}$, temos que este grupo de matrizes age de modo equivalente ao de simetrias de $\mathbb{Z}_m^n$.

[2] "equivalente" no sentido de ação de grupos: se ϕ é a aplicação que leva $v = (a_1, \ldots, a_n)$ em $e_{1a_1} + \ldots + e_{na_n}$, então $\phi((\sigma, \pi)(v)) = (\sigma, \pi)\phi(v)$. Observe que a representação é induzida da representação canônica de S_m em $\mathbb{R}^m$.

Analogamente ao grupo de automorfismos de $\mathcal{C}$ temos o grupo de simetrias que preserva o código. No entanto, este grupo não reúne necessariamente todas as isometrias de $\mathcal{C}$: podem existir isometrias do espaço métrico $(\mathcal{C}, d)$ que não são induzidas por simetrias do espaço ambiente.

Definição 8 *O grupo de todas as simetrias de $(\mathcal{C}, d)$ será denotado por $\mathbb{S}(\mathcal{C})$. Denotaremos por $\mathbb{S}(\mathcal{C}, A^n)$ o grupo de simetrias de (A^n, d) que preserva o código $\mathcal{C}$.*

Resumindo, temos

$$Aut\,(\mathcal{C}) \subset \mathbb{S}\,(\mathcal{C}, A^n) \subset \mathbb{S}(\mathcal{C})$$

Problemas envolvendo rotulamentos têm de levar em conta a distinção entre $\mathbb{S}\,(\mathcal{C}, A^n)$ e $\mathbb{S}(\mathcal{C})$. Esta distinção tem um interesse em si a partir do momento em que se consideram isometrias quaisquer entre códigos. Isto motivou a definição a seguir.

Definição 9 *[40] Seja $\mathcal{C}$ um código de (A^n, d). Dizemos que $\mathcal{C}$ é metricamente rígido quando os grupos $\mathbb{S}\,(\mathcal{C}, A^n)$ e $\mathbb{S}(\mathcal{C})$ são iguais.*

Quando o código é metricamente rígido pode-se concluir muita coisa a partir do grupo de simetrias de (A^n, d), mas o problema muda de figura no outro caso. Simetrias que não se estendem ao espaço ambiente aparecem nos códigos de Reed-Muller binários de primeira ordem, como mostraremos no Capítulo 4. O mesmo ocorre com os códigos de Reed-Solomon [40]. A importância destas simetrias reside no fato de que os rotulamentos cíclicos do código de Reed-Muller binário (e possivelmente dos q-ários) serem realizados por isometrias deste tipo.

Observamos também que os grupos de simetrias que são determinados e/ou utilizados neste trabalho possuem sempre a estrutura de um "wreath product" de um grupo finito por um grupo de permutações S_n.

Definição 10 *Seja G um grupo de n elementos e H um subgrupo de S_n. O "wreath product" de G por H é o produto semi-direto $H \ltimes G^n$ determinado pela ação canônica de H em G^n: se $g = (g_1, g_2, \ldots, g_n) \in G^n$ e $h \in H$, então*

$$h\,(g) = \left(g_{h^{-1}(1)}, \ldots, g_{h^{-1}(n)}\right).$$

Daí, se (h, g) e (h', g') pertencem a $H \ltimes G^n$, então

$$(h, g)\left(h', g'\right) = \left(hh', h'\,(g)\,g'\right).$$

Exemplos desta estrutura são os grupos de simetrias de espaços de Lee e de Hamming, e também os dos códigos de Reed-Muller de primeira ordem, que serão vistos no último capítulo.

1.3 Rotulamentos e Isometrias entre Módulos e Códigos

Rotulamentos são um maneira de conferir uma estrutura algébrica ao código usando grupos de simetrias. Esta estrutura tem ao menos duas utilidades: pode servir para estudar o código em si, ou também para usá-lo como ambiente de codificação. Exemplos deste último são os subcódigos de códigos de Reed-Muller definidos em [9, 17, 21]. Como já foi dito anteriormente, várias técnicas distintas de fornecer estruturas a códigos podem ser descritas como rotulamentos. O conceito de rotulamento que estamos usando aqui é o seguinte:

Definição 11 *Seja C um código e seja G um subgrupo de $\mathbb{S}(C)$. Diremos que G rotula o código C quando G agir livre e transitivamente em C. Os rotulamentos determinados por G são as aplicações*

$$\begin{array}{rccc} s_x: & G & \longrightarrow & C \\ & g & \longmapsto & gx \end{array}$$

indexadas por C.

A estrutura algébrica colocada em C é a do grupo G, e é dada por esta bijeção: definimos $yz = s_x\left(s_x^{-1}(y)\, s_x^{-1}(z)\right)$. Isto é o que acontece com os códigos propelineares, como veremos no capítulo 3. E é também o que ocorre com todas as isometrias entre anéis e códigos, ou módulos e códigos, que foram construídas como extensões da $\mathbb{Z}_4$-linearidade. Para entender como isto é feito nós voltaremos ao ponto de partida disto tudo, os códigos quaternários.

Definição 12 *A aplicação de Gray de $\mathbb{Z}_4$ em $\mathbb{Z}_2^2$ é dada por $\phi(0) = 00$, $\phi(1) = 01$, $\phi(2) = 11$, $\phi(3) = 10$. Sua extensão $\Phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$ feita coordenada a coordenada também é chamada de aplicação de Gray.*

Considerando a métrica de Hamming em $\mathbb{Z}_2^{2n}$, podemos tomar a função distância induzida em $\mathbb{Z}_4^n$ por esta isometria. A métrica d' induzida sobre $\mathbb{Z}_4^n$, $d'(u,v) = d_h(\Phi u, \Phi v)$, coincide com a métrica de Lee, e assim Φ é uma isometria de $(\mathbb{Z}_4^n, d_l)$ em $\left(\mathbb{Z}_2^{2n}, d_h\right)$. Esta isometria corresponde a uma ação de $(\mathbb{Z}_4^n, +)$ como grupo de simetrias de $\left(\mathbb{Z}_2^{2n}, d_h\right)$. Esta ação é facilmente determinada: para $u \in \mathbb{Z}_4^n$ e $v \in \mathbb{Z}_2^{2n}$, definimos $u(v) = \Phi\left(u + \Phi^{-1}(v)\right)$. Em particular, identificando $\mathbb{Z}_2^2$ com um quadrado centrado na origem em $\mathbb{R}^2$, vemos que $(\mathbb{Z}_4, +)$ corresponde ao grupo de rotações deste quadrado. Por extensão, o grupo $(\mathbb{Z}_4^n, +)$ corresponde a um grupo de rotações do "$2n$-cubo" $\mathbb{Z}_2^{2n}$. Em termos de rotulamentos, o grupo rotulador é $(\mathbb{Z}_4^n, +)$, e o ponto inicial é a origem – na notação da definição 11, $\Phi(u) = s_0(u) = u(0)$.

Esta correspondência entre uma isometria do anel $\mathbb{Z}_4^n$ sobre $\mathbb{Z}_2^{2n}$ e uma ação do grupo aditivo deste $\mathbb{Z}_4$-módulo em $\mathbb{Z}_2^{2n}$ funciona para quaisquer R-módulos. No lema abaixo nós fornecemos os detalhes.

Lema 1 *Sejam R anel, M um R-módulo dotado de um peso w, (X,d) um espaço métrico, e seja C um código de X. Então os espaços (M,w) and (C,d) são isométricos se e só se o grupo aditivo de M, $G = (M,+)$, é isomorfo a um subgrupo de $\mathbb{S}(C)$ que age livre e transitivamente.*

Demonstração. Seja $\phi : (M, w) \to (\mathcal{C}, d)$ uma isometria. Dados x em $\mathcal{C}$ e m em G, definimos $m(x) = \phi(m + \phi^{-1}(x))$. Isto define uma ação de G em X, pois

$$\begin{aligned} m(n(x)) &= m\left(\phi\left(n + \phi^{-1}(x)\right)\right) \\ &= \phi\left(m + \phi^{-1}\left(\phi\left(n + \phi^{-1}(x)\right)\right)\right) \\ &= \phi\left(m + n + \phi^{-1}(x)\right) \\ &= (m + n)(x) \end{aligned}$$

Além disso, como ϕ é isometria,

$$\begin{aligned} d(m(x), m(y)) &= d\left(\phi(m + \phi^{-1}(x)), \phi(m + \phi^{-1}(y))\right) \\ &= w\left(m + \phi^{-1}(x) - \left(m + \phi^{-1}(y)\right)\right) \\ &= w\left(\phi^{-1}(x) - \phi^{-1}(y)\right) \\ &= d(x, y). \end{aligned}$$

Finalmente, a ação é transitiva, pois $\phi(M) = X$, e $m(\phi(0)) = \phi(m + 0) = \phi(m)$ - ou seja, $G(0) = X$. E é livre pois é transitiva e $|M| = |X|$.

Reciprocamente, se G é um grupo de simetrias abeliano que age livre e transitivamente em $\mathcal{C}$, tome um ponto $x \in X$ qualquer e defina sobre G a métrica $d_x(g, h) = d(g(x), h(x))$. Esta métrica é invariante sob G. Se M é um módulo tal que $(M, +)$ é isomorfo a G, seja $\alpha : (R, +) \to G$ um tal isomorfismo; segue que $d_\alpha(m, n) = d_x(\alpha(m), \alpha(n))$ define uma métrica sobre M e um peso $w_\alpha(m) = d_\alpha(m, 0)$, e que a aplicação $\phi : (M, w) \to (\mathcal{C}, d)$ definida como $\phi(m) = \alpha(m)(x)$ é uma isometria.

Deste modo, podemos investigar a existência de isometrias entre R-módulos e códigos via o estudo do grupo de simetrias do código em questão.

Capítulo 2

Rotulamentos em espaços de Lee

2.1 Introdução

Neste capítulo vamos tratar de rotulamentos em espaços de Lee. Estes espaços podem ser definidos como quocientes de grafos sobre $\mathbb{Z}^n$, e isto permite relacionar parametrizações em espaços de Lee com ladrilhamentos de $\mathbb{R}^n$. Os principais resultados deste capítulo são a construção de um rotulamento não-abeliano para uma família de espaços de Lee, e uma descrição completa dos códigos perfeitos em espaços de Lee bidimensionais.

Na primeira e segunda seções são colocados os conceitos básicos – grafos sobre reticulados, grafos e espaços métricos quocientes, ladrilhamentos – e são desenvolvidos alguns resultados gerais sobre ladrilhamentos de espaços quocientes. Basicamente, nós estudamos ladrilhamentos do quociente induzidos do espaço original. Um dos resultados mais interessantes é a determinação de condições suficientes para que todos os ladrilhamentos de um espaço métrico quociente sejam induzidos do espaço original.

Na terceira seção estudamos os códigos perfeitos em dimensão 2. A classificação que apresentamos segue as idéias geométricas de [20], e o que acrescentamos é uma construção mais rigorosa destes códigos. Algebricamente, isto é a construção A de Conway/Sloane [11]: toma-se em $\mathbb{R}^n$ a pré-imagem do código C pela projeção canônica de $\mathbb{Z}^n$ sobre $\mathbb{Z}_m^n$. Geometricamente, consideramos o problema no toro e não em $\left(\mathbb{Z}_q^2, d_l\right)$, e depois trabalhamos no plano mesmo para enfim projetar as soluções (reticulados) no toro. Deste modo podemos concluir que para cada $n > 1$ existem apenas dois códigos perfeitos em cada espaço $\left(\mathbb{Z}_q^2, d_l\right)$, onde $q = m\left(2n^2 + 2n + 1\right)$, e que estes são equivalentes.

Na última seção nós construímos parametrizações não-abelianas de uma família de espaços de Lee. Esta construção é motivada pelo conceito da *G-linearidade*, na qual o primeiro passo é a determinação de um rotulamento do espaço ambiente, e por trabalhos anteriores [19, 13, 30]. Nestes nós mostramos que o único grupo rotulador abeliano é o das translações, e por isso a necessidade de que outros rotulamentos utilizem grupos não-comutativos. A idéia é obter códigos como órbitas de subgrupos do grupo rotulador (a G-linearidade será estudada mais detalhadamente no próximo capítulo).

Os resultados obtidos sobre rotulamentos de grafos quocientes ainda podem ser utilizados em outros contextos, como em códigos esféricos [14]. Neste caso, os reticulados são $\mathbb{Z}^n$ e Λ, um subreticulado de $\mathbb{Z}^n$ de posto n que possui uma base ortonormal. Nestas condições podemos mergulhar o toro n-dimensional $T^n = \mathbb{R}^n/\Lambda$ isometricamente na esfera S^{2n-1}. O código esférico $\mathcal{C}$ é a imagem do reticulado $\mathbb{Z}^n$, e estes pontos correspondem de modo natural aos elementos do grupo $\mathbb{Z}^n/\Lambda$. Este grupo tem uma representação no grupo de matrizes ortogonais que serve como rotulamento do código $\mathcal{C}$. O grafo quociente se realiza sobre a esfera com geodésicas (sobre o toro) como arestas, e em alguns casos a distância euclidiana pode ser aproximada pela distância no grafo. Também podem ser utilizados em códigos sobre uma região fundamental de um reticulado, como em [24] e [34], onde a métrica do grafo é uma aproximação da métrica euclidiana restrita aos pontos do reticulado. Talvez sejam um modo de trabalhar com reticulados com pouca estrutura algébrica.

Grande parte deste capítulo está nos artigos "Graphs, Tesselations and Perfect Codes on Flat Tori" [12], feito por Sueli Costa, Marcelo Muniz, Edson Agustini e Reginaldo Palazzo Júnior, e em "Labelings of Lee and Hamming spaces" [28], feito com Sueli Costa.

2.2 Grafos sobre Toros

Definição 13 *Um reticulado Λ em $\mathbb{R}^n$ é um subgrupo discreto de $(\mathbb{R}^n, +)$. O posto de Λ é a dimensão do subespaço vetorial real gerado por Λ.*

Definição 14 *Seja Λ um reticulado e $\beta = \{v_1, \ldots, v_k\}$ um conjunto de vetores não-nulos que contém uma base de Λ. O grafo associado ao par (Λ, β) tem por vértices os pontos de Λ e por arestas os pares (u, v) tais que $u - v$ pertence a $\beta \cup -\beta$.*

Dito de outro modo, o grafo do par (Λ, β) é o grafo de Cayley associado ao grupo Λ e a seu conjunto gerador $\beta \cup -\beta$. A definição de grafo de Cayley usada neste trabalho é a que segue:

Definição 15 *Seja G um grupo, e seja $S \subset G$ um conjunto de geradores de G que é simétrico ($S = S^{-1}$) e não contém a identidade do grupo. O grafo de Cayley associado a G e S tem por vértices os elementos de G, e suas arestas são os (g, h) tais que $h^{-1}g$ pertence a S.*

Os espaços métricos associados têm por função distância a métrica do grafo.

Definição 16 *Seja Γ um grafo conexo. Um caminho α em Γ é uma sequência de vértices $v_1, v_2, \ldots, v_n$ tal que cada vértice se encontra ligado por uma aresta ao seguinte. O comprimento $l(\alpha)$ de um caminho $\alpha = (v_i)_{i=1,\ldots,n}$ é o número de arestas percorridas, ou seja, $n-1$. A função distância d_Γ é definida por: $d_\Gamma(a, b) = \min\{l(\alpha);\ \alpha$ é um caminho de a a $b\}$.*

Pode-se verificar que d_Γ é realmente uma métrica sobre o grafo Γ. Os espaços de Lee e espaços de Hamming são exemplos clássicos de espaços métricos associados a grafos de Cayley sobre os respectivos alfabetos. Os de Lee sobre $\mathbb{Z}_m^n$ têm conjunto gerador $S = \{\pm e_i; i = 1, \ldots, n\}$, os de

Hamming sobre A^n o conjunto $S = \{\pm a_i e_i; a_i \in A - \{0\}, i = 1, \ldots, n\}$. Esta função distância também transforma em espaços métricos os grafos (Λ, β). Todas as construções desta seção vêm de espaços como estes, como os próximos dois exemplos.

Exemplo 1 *Considere o reticulado $\mathbb{Z}^n$. O grafo associado à base canônica de $\mathbb{Z}^n$ é usualmente identificado com o próprio reticulado. Suas arestas correspondem a segmentos de reta que unem pontos u, v tais que $||u - v|| = 1$.*

Exemplo 2 *Considere o reticulado A_2, que é gerado por $(1,0)$ e $\left(\frac{1}{2}, \frac{\sqrt{3}}{2}\right)$. Identificando $\mathbb{R}^2$ com o plano complexo $\mathbb{C}$, tome β como o conjunto de raízes sextas de 1, ou seja, $\beta = \{\exp(k2\pi i/6), k = 0, 1, \ldots, 5\}$. O grafo correspondente é regular com valência 6. Este grafo é o ponto de partida para a construção de espaços sobre quocientes do anel de Eisenstein-Jacobi [25].*

Nós estamos basicamente interessados em conectar problemas em espaços de Lee e em $\mathbb{R}^n$. Neste sentido, vamos considerar algumas estruturas quocientes e as relações entre isometrias do espaço quociente e isometrias do espaço original.

Definição 17 *Seja Γ um grafo conexo e G um grupo de automorfismos de Γ. O grafo quociente Γ/G tem por vértices as órbitas de Γ por G. Dois vértices $\overline{x} = \Gamma x$ e $\overline{y} = \Gamma y$ são ligados se e só se (x, gy) é aresta de Γ para algum g de G.*

Para as aplicações, vamos requerer que tanto o grafo Γ quanto o quociente Γ/G não tenham laços. Se Γ não possui laços, então Γ/G também não terá, desde que o grupo G não tenha dois vértices adjacentes na mesma órbita. Um exemplo geral é o seguinte: seja (Λ, β) um grafo sobre o reticulado Λ, e seja Λ' um subreticulado de Λ, ambos de posto máximo, de modo que Λ' não possua nenhum vetor de β. Tomando Λ' como o grupo G da última definição, construímos um grafo sobre Λ/Λ'. Este é o grafo associado ao conjunto gerador $\overline{\beta} = \beta + \Lambda'$ de Λ/Λ', e se realiza sobre o toro $\mathbb{R}^n/\Lambda'$.

Exemplo 3 *Cada espaço de Lee $(\mathbb{Z}_m^n, d_l)$ corresponde a um quociente destes. Aqui, $\Lambda = \mathbb{Z}^n$, β é a base canônica, e $\Lambda' = m\mathbb{Z}^n$.*

Exemplo 4 *Na métrica de Mannheim, usam-se ideais do anel de Gauss como subreticulados. O grafo é o $(\mathbb{Z}^2, \{e_1, e_2\})$. Os ideais do anel de Gauss correspondem a reticulados com bases ortogonais do tipo $\beta = \{(a, b), (-b, a)\}$*

2.3 Ladrilhamentos e Códigos

Problemas de códigos em espaços de Lee podem ser relacionados a problemas de ladrilhamentos em $\mathbb{R}^n$. Nesta parte do trabalho colocamos resultados sobre ladrilhamentos necessários ao estudo de códigos perfeitos e à construção dos rotulamentos de espaços de Lee. O primeiro resultado mostra como se pode calcular um subgrupo de isometrias de um espaço quociente via o espaço original.

Teorema 2 *Seja G um grupo discreto*[1] *de isometrias de M. Seja M/G o espaço quociente, isto é, o espaço das órbitas de G em M. Então*

(i) A função $d'(\overline{x},\overline{y}) = \min_{g\in G} d(gx,y)$ é uma métrica em M/G;

(ii) Seja $N(G)$ o normalizador de G no grupo de simetrias de M. Então, se f pertence a $N(G)$, a aplicação $\overline{f} : M/G \to M/G$ definida por $\overline{f}(\overline{x}) = \overline{f(x)}$ é uma isometria de M/G. Isto define um homomorfismo $P : N(G) \to \mathbb{S}(M/G)$ que tem núcleo igual a G.

Demonstração. O item (i) é facilmente verificado (ver [13, 30]). Quanto ao item (ii), tome uma simetria $g \in N(G)$; a aplicação $\overline{g}$ dada por $\overline{g}(\overline{x}) = \overline{g(x)}$ é simetria de M/G, pois

$$d_{M/G}(\overline{gx},\overline{gy}) = \min_{h\in G} d(gx,hgy) = \min_{h\in G} d(x,g^{-1}hgy) = \min_{h\in G} d(x,hy) = d_{M/G}(\overline{x},\overline{y}),$$

e a associação $g \longmapsto \overline{g}$ define um homomorfismo de $N(G)$ em $\mathbb{S}(M/G)$ com núcleo G. ■

Os grupos de simetria dos espaços de Lee podem ser calculados desta forma; neste caso, a aplicação P é sobrejetora, a menos dos casos $\mathbb{Z}_2^{2n}$ e $\mathbb{Z}_4^n$. Outro conceito de que faremos uso é o de ladrihamentos. Os códigos geometricamente uniformes em espaços de Lee correspondem a ladrilhamentos do toro, e em boa parte dos casos, a ladrilhamentos de $\mathbb{R}^n$. Observamos que não vamos considerar aqui ladrilhamentos que não sejam dados por grupos discretos. Portanto, onde estiver escrito "ladrilhamento", leia-se ladrilhamento dado por um grupo discreto de isometrias.

Definição 18 *Seja G um grupo discreto de isometrias de um espaço métrico M. Um subconjunto D de M é uma região fundamental associada a G se:*

(i) $\bigcup_{g\in G} gD = M$;

(ii) $\mathrm{int}(D) \cap int(gD) \neq \varnothing \iff g = 1$. *($\mathrm{int}(D)$ é o interior de D)*

(iii) $\mathrm{int}(D) \neq \varnothing$.

O recobrimento de M dado por cópias de D (os ladrilhos) sob a ação de G é chamado um ladrilhamento de M associado a G.

Lema 2 *[18]A região $D(x) = \{y \in M; d(x,y) \leq d(x,gy), \forall g \in G\}$ é uma região fundamental para G, chamada de* domínio de Dirichlet de x, *ou também de* região de Voronoi de x.

[1] por grupo discreto entendemos um grupo de simetrias cujas órbitas são discretas (subconjuntos fechados que só possuem pontos isolados)

Um ladrilhamento de M pode ser a base para ladrilhamentos de quocientes de M; reciprocamente, recobrimentos de um quociente podem ser levantados ao espaço M, desde que satisfaçam algumas condições. Estas condições de compatibilidade são o objeto dos próximos resultados.

Teorema 3 *Seja M espaço métrico, G um subgrupo discreto de isometrias, e $M = \bigcup_{g\in G} gD$ um ladrilhamento de M associado a G. Então, se H é subgrupo normal de G, esse ladrilhamento induz um outro do espaço M/H, com grupo associado G/H.*

Demonstração. Seja $p : M \to M/H$ a projeção canônica, e tome $\overline{D} = p(D)$ como sendo o ladrilho fundamental. Primeiro, note que o grupo G/H age como grupo de simetrias em M/H, pois H é normal em G (Teorema 2). Além disso, $p(gD) = \overline{g}\overline{D}$. Isso pode ser verificado apenas com as definições de p e de $\overline{g}$.

É facil ver que $M/H = \bigcup_{\overline{g}\in G/H} \overline{g}\overline{D}$. Seja $\overline{x} \in M/H$. O ponto x, que é uma das pré-imagens de $\overline{x}$, pertence a algum domínio gD. Então $\overline{x} \in p(gD) = \overline{g}\overline{D}$.

Quanto à intersecção de interiores de regiões, observamos antes que a projeção p é uma aplicação de recobrimento; portanto, é contínua e aberta, e $p(int(A)) = int(p(A))$, para qualquer subconjunto A de M. Em particular, $p(int(gD)) = int(\overline{g}\overline{D})$.

Suponha que $int(\overline{g}\overline{D}) \cap int(\overline{D}) \neq \varnothing$. Isto é o mesmo que $p(int(gD)) \cap p(int(D)) \neq \varnothing$. Por sua vez, $int(gD) = g(int(D))$, pois g é um homeomorfismo. Isto implica na existência de x e y em $int(D)$ e h em H tais que $hx = gy$. Ou seja, $int(gD) \cap int(hD) \neq \varnothing$. Como gD e hD são duas regiões de um ladrilhamento em M, $gD = hD$ e $g = h$. Logo, $\overline{g}\overline{D} = \overline{hD} = \overline{D}$. Ou seja, se $int(\overline{g}\overline{D}) \cap int(\overline{D}) \neq \varnothing$, então $\overline{g}\overline{D} = \overline{D}$. Com isto demonstramos que $M/H = \bigcup_{\overline{g}\in G/H} \overline{g}\overline{D}$ é um ladrilhamento de M/H. ■

Este teorema permite construir ladrilhamentos do quociente a partir de ladrilhamentos de M.

Exemplo 5 *Considere o reticulado $\mathbb{Z}^n$ em $\mathbb{R}^n$. O grupo de simetrias euclidianas deste reticulado é isomorfo a $\mathbb{Z}^n \rtimes (\mathbb{Z}_2^n \rtimes S_n)$ [11]. Seja T o toro $\mathbb{R}^n/m\mathbb{Z}^n$. Então qualquer ladrilhamento de $\mathbb{R}^n$ feito por um grupo que contém $m\mathbb{Z}^n$ como subgrupo normal dá origem a um ladrilhamento deste toro. Por exemplo, o grupo $\mathbb{Z}_m^n$ ladrilha T tendo como região fundamental um quadrado unitário.*

A recíproca é verdadeira quando o homomorfismo $\mathbb{S}(M) \to \mathbb{S}(M/G)$ é sobrejetor: assim, pode-se estudar os ladrilhamentos de M/G a partir dos de M.

Teorema 4 *Seja M espaço métrico e H um subgrupo discreto de isometrias, $N(H)$ e M/H como antes, $p : M \to M/H$ a projeção. Seja $\overline{G}$ um subgrupo discreto de simetrias de M/H, e seja $M/H = \bigcup_{\overline{g}\in\overline{G}} \overline{g}\overline{D}$ um ladrilhamento de M/H. Se $\mathbb{S}(M/H) \cong N(H)/H$, então existem D em M e G subgrupo de $N(H)$ tais que $\overline{G} = G/H$, $\overline{D} = p(D)$, e $M = \bigcup_{g\in G} gD$ é um ladrilhamento. Além disso, o ladrilhamento de M/H por $\overline{D}$ é induzido pelo anterior.*

Demonstração. Para o grupo G, basta usar o fato de que $\mathbb{S}(M/H) = N(H)/H$. Daí sai que $\overline{G} = G/H$ para algum $G < N(H)$ (Teorema 2). Para a região D, seja D um domínio contido em $p^{-1}(\overline{D})$ tal que $p|_D$ seja bijetora.

Primeiro, mostremos que $M = \bigcup_{g\in G} gD$.

Note que $p(gD) = \overline{g}\overline{D}$. De fato, $\overline{g}\overline{D} = \{\overline{g}\overline{x}; \overline{x} \in \overline{D}\} = \{\overline{g}\overline{x}; x \in D\}$, pois p é bijeção entre D e $\overline{D}$. Por sua vez, $p(gD) = \{\overline{g}\overline{x}; x \in D\} = \overline{g}\overline{D}$.

Quanto às imagens inversas, afirmamos que

$$p^{-1}(\overline{g}\overline{D}) = \bigcup_{h\in H} hgD.$$

Seja $x \in p^{-1}(\overline{g}\overline{D})$. Então

$$\begin{aligned} \overline{x} \in \overline{g}\overline{D} &\Leftrightarrow \overline{x} = \overline{g}\overline{y}, y \in D \\ &\Leftrightarrow hx = gy, \text{para algum } h \in H \\ &\Leftrightarrow x \in h^{-1}gD, \end{aligned}$$

o que mostra um lado da inclusão. O outro é claro, pois $p(hgD) = p(gD) = \overline{g}\overline{D}$, e temos a igualdade.

Isto permite concluir esta parte, pois

$$M = p^{-1}(\bigcup_{\overline{g}\in\overline{G}} \overline{g}\overline{D}) = \bigcup_{\overline{g}\in\overline{G}} p^{-1}(\overline{g}\overline{D}) = \bigcup_{\overline{g}\in\overline{G}} \bigcup_{h\in H} hgD \subset \bigcup_{g\in G} gD \subset M.$$

Quanto às intersecções de regiões, vamos partir em dois casos.

Primeiro, suponha que $h \in H$, e que a intersecção de $int(D)$ com $int(hD)$ não é vazia. Seja x um ponto da intersecção. Então existe $y \in D$ tal que $x = hy$, e temos $p(x) = p(hy) = p(y)$. Mas p restrita a D é bijetora, e segue daí que $x = y$ e $h = id$.

Seja agora $g \in G$ qualquer. Suponha que $int(D) \cap int(gD) \neq \varnothing$. Então existem $x, y \in int(D)$ tais que $x = gy$. Aplicando p, obtemos

$$p(int(D)) \cap p(int(gD)) = int(\overline{D}) \cap int(\overline{g}\overline{D}) \neq \varnothing$$

Como temos um ladrilhamento em M/H, $\overline{D} = \overline{g}\overline{D}$, ou seja, $g \in H$. Com isto voltamos ao caso anterior, e $g = id$. Logo, se $int(D) \cap int(gD) \neq \varnothing$, $g = id$. Isto mostra que $M = \bigcup_{g\in G} gD$ é um ladrilhamento de M. ∎

Estes últimos resultados conectam problemas de ladrilhamento em M e em seus quocientes. Nas próximas seções utilizaremos isso para resolver problemas em espaços de Lee via ladrilhamentos de $\mathbb{R}^n$.

2.4 Códigos Perfeitos em espaços de Lee

Códigos perfeitos são partições do espaço métrico M em bolas de mesmo raio. Isto é, cada ponto de M está em uma única bola $B_r(c)$, para algum ponto c do código. Pela própria definição, é de se esperar que hajam limitações à existência destes códigos.

Os códigos perfeitos lineares em espaços de Hamming sobre corpos finitos são conhecidos, sendo [27] uma boa referência sobre o assunto. Há uma família infinita, os códigos de Hamming $\mathcal{H}_{m,q}$, que têm parâmetros $\left[\frac{q^m-1}{q-1}, \frac{q^m-1}{q-1} - m, 3\right]$. Existem mais dois códigos, o código de Golay binário $\mathcal{G}_{23}$, com parâmetros $[23, 12, 7]$, e o código de Golay ternário $\mathcal{G}_{11}$, que é um código $[11, 6, 5]$. Observe que só há três distâncias mínimas possíveis: 3, 5 e 7. Todos os códigos perfeitos lineares são equivalentes, isto é, todos estão na mesma órbita sob o grupo de automorfismos do espaço ambiente [27, Captulo 20].

A situação no caso dos espaços de Lee é inconclusiva. Há resultados de existência, mas não se sabe se a lista de códigos perfeitos está fechada, ou em quantas classes de equivalência se particionam os já conhecidos. Os exemplos conhecidos são: uma família de códigos corretores de 1 erro em $\left(\mathbb{Z}^n_{2m+1}, d_l\right)$, que consiste dos hiperplanos definidos pela equação $x_1+2x_2+\ldots+nx_n = 0$, e uma de códigos bidimensionais corretores de t erros, em $\left(\mathbb{Z}^2_{2t^2+2t+1}, d_l\right)$, dada pelas retas $(2t+1)\,x_1 + x_2 = 0$. Todos estes são apresentados em [20], sendo que as demonstrações no caso dos códigos corretores de um erro são detalhadas em [5] e posteriormente em [35, 36]. Até o momento, são estes os únicos resultados positivos sobre códigos perfeitos em espaços de Lee. Todos os demais são negativos, e uma conjetura já colocada em [20] (em 1967) é que não existam códigos perfeitos de raio maior que 1 em espaços de Lee de dimensão maior que 2.

A primeira construção destes códigos explora conexões entre os códigos lineares perfeitos e ladrilhamentos de $\mathbb{R}^n$ por reticulados. (o mesmo funciona para qualquer espaço métrico proveniente de um grafo sobre um reticulado). Nesta seção nós demonstramos a equivalência entre uma classe de ladrilhamentos de $\mathbb{R}^n$, códigos perfeitos em espaços de Lee e ladrilhamentos em toros. Como aplicação, mostramos que basicamente não há outros códigos lineares perfeitos em dimensão dois além dos já conhecidos. Há apenas dois em cada espaço $\left(\mathbb{Z}^2_{k(2t^2+2t+1)}, d_l\right)$ e eles são equivalentes.

Para buscar códigos perfeitos lineares vamos procurar subreticulados de $\mathbb{Z}^n$. Por isso, é interessante particularizar o estudo da última seção para grupos G que sejam reticulados.

Teorema 5 *Sejam $\alpha = \{v_1, v_2, \ldots, v_n\}$ e $\beta = \{w_1, w_2, \ldots, w_n\}$ bases de $\mathbb{R}^n$, Λ_a e Λ_β os reticulados (e grupos de translações) associados. Seja $\mathbb{R}^n = \bigcup_{g\in\Lambda_\alpha} gD$ um ladrilhamento de $\mathbb{R}^n$ com o ladrilho D. Então existe um ladrilhamento do toro $T_\beta = \frac{\mathbb{R}^n}{\Lambda_\beta}$ induzido por esse, com o ladrilho correspondente, se e só se Λ_α é subreticulado de Λ_β.*

Demonstração. Se Λ_α é subreticulado, podemos usar o Teorema 3. Por outro lado, suponha que o ladrilhamento de $\mathbb{R}^n$ induz um em T_β. Então cada $w_i D$ tem de ser igual a uma gD, com $g \in \Lambda_\alpha$. Se isto não acontece, temos uma sobreposição $(w_i - \widetilde{w}_i)D \cap D \neq \varnothing$, com $\widetilde{w}_i$ sendo a parte inteira de w_i escrito na base α. Esta sobreposição dá origem a uma sobreposição de ladrilhos em T_β. ■

Para iniciar nosso estudo dos códigos perfeitos em espaços de Lee vamos considerar o grafo canônico sobre $\mathbb{Z}^n$ (dado pelo conjunto gerador $S = \{\pm e_i, i = 1, \ldots, n\}$. A métrica associada coincide com a norma da soma dos módulos, $||u|| = \sum |u_i|$. Seja Λ um subreticulado de $\mathbb{Z}^n$, e considere o grafo quociente em $\mathbb{Z}^n/\Lambda$. Se a norma mínima de um vetor de Λ é r, então a projeção $p : \mathbb{Z}^n \longrightarrow \mathbb{Z}^n/\Lambda$ é uma r-isometria local. Portanto, existirão códigos perfeitos com raio $s < r/2$ em $\mathbb{Z}^n/\Lambda$ (parametrizados por grupos de simetria) se e só se existirem tais códigos em $\mathbb{Z}^n$. Por sua vez, pode-se associar às bolas de raio s em $\mathbb{Z}^n$ regiões convenientes de $\mathbb{R}^n$. Para isso, tome a região de Dirichlet (em relação a $\mathbb{Z}^n$) em torno de cada ponto da bola, e seja $R(s, v)$ a união destas pequenas regiões (ver Figura 1 abaixo para $n = 2$ e $s = 3$). Ou seja, se $Q(w)$ é o cubo unitário centrado em w, $Q(w) = \{u \in \mathbb{R}^2; |w_i - u_i| \leq 1/2\}$, a região associada à bola $B_s(v)$ é dada por $R(s, v) = \bigcup_{\substack{w \in \mathbb{Z}^2 \\ ||w-v|| \leq s}} Q(w)$. Chamaremos esta região de poliedro de Voronoi de v com raio s.

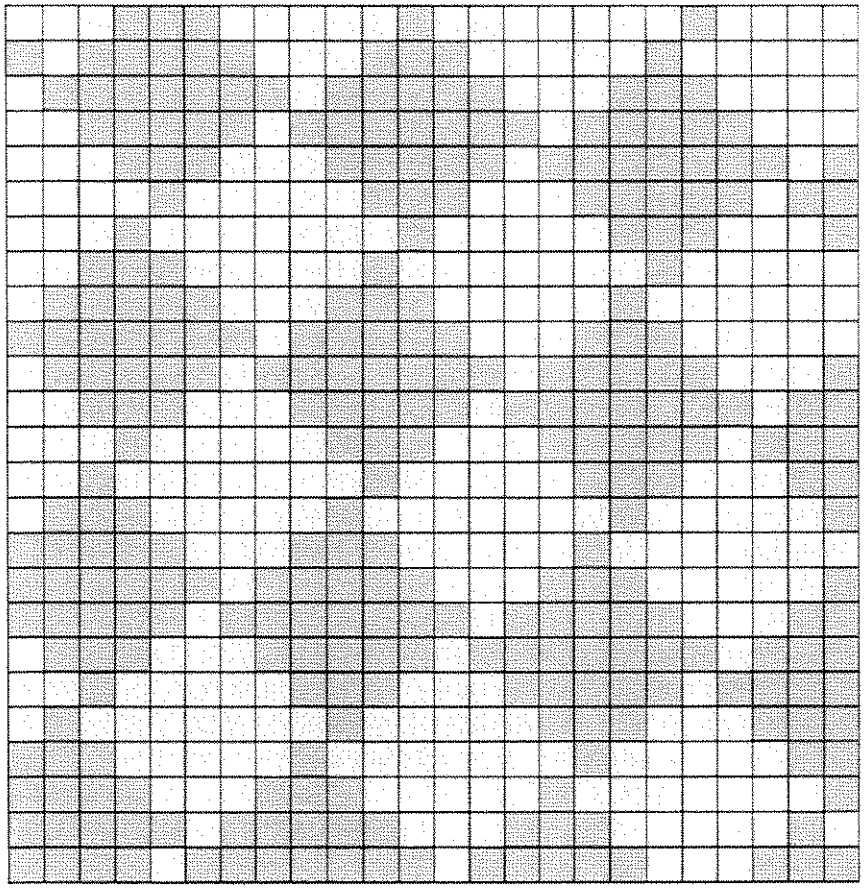


FIGURA 1 O código perfeito $t(4,3)$ no espaço de Lee $\left(\mathbb{Z}_{25}^2, d_l\right)$ e correspondente ladrilhamento no plano pelo reticulado $\Lambda = \langle (4,3), (-3,4) \rangle$ com região fundamental $R(3,0)$.

Intuitivamente, é de se esperar que um código perfeito de raio s em $\mathbb{Z}^n$ determine um ladrilhamento de $\mathbb{R}^n$ pelos poliedros $R(s,v)$, com v percorrendo o código, e reciprocamente. Isto é verdadeiro, e é o que é demonstrado no lema a seguir.

Lema 3 *Para cada código perfeito de raio s em $\mathbb{Z}^n$ existe um ladrilhamento correspondente pelas regiões $R(s,v)$ centradas em pontos do código, e reciprocamente.*

Demonstração. Seja $\mathcal{C}$ um código perfeito de raio r em $\mathbb{Z}^n$, e seja G um grupo de simetrias que parametriza este código. Ou seja, $\mathcal{C} = G(v)$, onde v é um ponto arbitrário de $\mathcal{C}$.

Como $\mathcal{C}$ é perfeito, $\mathbb{Z}^n = \bigcup_{v \in \mathcal{C}} B_s(v)$. Seja $R(s,v)$ o poliedro de Voronoi associado à bola $B_s(v)$. Note que $\mathbb{R}^n = \bigcup_{v \in \mathcal{C}} R(s,v)$, pois $R(s,v) = \bigcup_{a \in B_s(v)} \{w \in \mathbb{R}^n; |w_i - a_i| \leq 1/2, i = 1, \ldots, n\}$. Dado $w \in \mathbb{R}^n$, existem $a_1, \ldots, a_n$ inteiros tais que $|w_i - a_i| \leq 1/2$, $i = 1, \ldots, n$. Como $\mathcal{C}$ é perfeito, existe um único $v \in \mathcal{C}$ tal que $(a_1, \ldots, a_n) \in B_s(v)$. E w está em $Q((a_1, \ldots, a_n))$, que está contido em $R(s,v)$.

Agora verificaremos que $int(R(s,u)) \cap int(R(s,v))$ é vazio se $u \neq v$. Pela definição destas regiões, e por u e v serem elementos de $\mathbb{Z}^n$, temos que $int(R(s,u)) \cap int(R(s,v)) \neq \varnothing$ se e só se $R(s,u) \cap R(s,v)$ contém um quadrado $Q(w)$. Neste caso é óbvio que o código não é perfeito, pois $w \in B_s(u) \cap B_s(v)$. Segue que $int(R(s,u)) \cap int(R(s,v)) = \varnothing$.

Finalmente, o grupo G. Sabemos que G é um grupo de simetrias euclidianas [13]. Logo, $g \in G$ leva a região $R(s,v)$ na região $R(s,gv)$ – basta ver a definição destas, e lembrar que G permuta os centros das bolas $B_s(u)$. Portanto, as regiões $R(s,v)$ são regiões fundamentais de G, e $\mathbb{R}^n = \bigcup_{g \in G} R(s,gv) = \bigcup_{g \in G} gR(s,v)$ para um $v \in \mathcal{C}$ qualquer fixado.

Reciprocamente, suponha que $\mathbb{R}^n = \bigcup_{g \in G} R(s,gv)$ e que $int(R(s,gv)) \cap int(R(s,hv))$ é vazio se $g \neq h$. Então é claro que o código $\mathcal{C} = G(v)$ é perfeito: dado qualquer vetor de coordenadas inteiras, este só pode estar no interior de uma $R(s,gv)$, ou seja, ele pertence a $B_s(gv)$. Isto termina a demonstração. ■

Deste modo, podemos dizer que existe um código perfeito com raio s, rotulado por um grupo $\overline{G}$, em $\mathbb{Z}^n/\Lambda$, se e só se existe um grupo G que ladrilhe $\mathbb{R}^n$ com $R(s,v)$.

Em particular, já podemos concluir o seguinte:

Teorema 6 *Seja $(\mathbb{Z}_m^n, d_l)$ o espaço de Lee sobre $\mathbb{Z}_m^n$. Então, existe um código perfeito de raio r em $\mathbb{Z}_m^n$ rotulado por um grupo de simetrias, com $s \leq m/2$, se e só se existir um ladrilhamento de $\mathbb{R}^n$ pelas regiões $R(s,v)$.*

De fato, aqui Λ é $m\mathbb{Z}^n$, e os vetores de norma mínima são os vetores me_i.

2.4.1 Códigos Perfeitos Bidimensionais

Finalmente, vamos usar estes resultados para obter todos os códigos de Lee perfeitos e lineares em dimensão 2. Para isto precisaremos de mais um teorema sobre ações de grupos discretos, cuja demonstração pode ser vista em [18, Teorema 6.2, pp.104-105].

Teorema 7 *[18]Seja G um grupo discreto de isometrias agindo em (M,d), e seja H um subgrupo de índice finito em G, de modo que $G = g_1H \cup \ldots \cup g_mH$. Se D é um domínio fundamental de G, então $D' = \bigcup_{i=1}^{n} g_iD$ é um domínio fundamental de H.*

Observe que a região $R(s,0)$ é montada a partir de regiões de Dirichlet do reticulado $\mathbb{Z}^2$. Deste modo, o que buscaremos são subreticulados de $\mathbb{Z}^2$ tais que o domínio D' definido acima coincida com $R(s,0)$.

Teorema 8 *Os únicos reticulados que ladrilham $\mathbb{R}^2$ com o domínio fundamental $R(s,0)$ são* $\Lambda_1 = \langle\{(s,s+1),(-s-1,s)\}\rangle$ *e* $\Lambda_2 = \langle\{(s+1,s),(-s,s+1)\}\rangle$.

Demonstração. Primeiro, mostremos que estes reticulados têm $R(s,0)$ como região fundamental. As regiões $R(s,v)$ são uniões de regiões de Dirchlet do grupo $\mathbb{Z}^2$, e $R(s,0)$ ainda pode ser escrita como $R(s,0) = \cup_{v\in R(s,0)\cap\mathbb{Z}^2} Q(v)$, onde $Q(v)$ é o quadrado unitário centrado em v. Usando o Teorema 7, vemos que basta mostrar que $R(s,0)\cap\mathbb{Z}^2$ é um sistema completo de representantes de $\mathbb{Z}^2/\Lambda_1$ (e $\mathbb{Z}^2/\Lambda_2$).

Consideremos Λ_1 primeiro. $R(s,0)\cap\mathbb{Z} = \{(u_1,u_2)\in\mathbb{Z}; ||(u_1,u_2)|| = |u_1|+|u_2|\leq s\}$. Dado um ponto u de Λ_1, $u = a_1(s,s+1)+a_2(-s-1,s)$, temos

$$|u_1|+|u_2| \geq ||u||_e = \sqrt{(|a_1|+|a_2|)(2s^2+2s+1)} \geq \sqrt{(2s^2+2s+1)} > (s+1),$$

o que mostra que o único ponto de Λ_1 em $R(s,0)$ é a origem.

O reticulado quociente $\mathbb{Z}^2/\Lambda_1$ possui $|\det A|$ elementos, onde A é a matriz com vetores coluna $(s,s+1)$ e $(-s-1,s)$. Como $\det A = 2s^2+2s+1$, e a bola de raio s na métrica da soma dos módulos possui este mesmo número de pontos, conclui-se que $R(s,0)\cap\mathbb{Z}^2$ é um sistema completo de representantes de $\mathbb{Z}^2/\Lambda_1$. Portanto, $R(s,0)$ é uma região fundamental de Λ_1.

Quanto a Λ_2, note que este reticulado é obtido de Λ_1 pela reflexão T dada por $(x,y)\mapsto(y,x)$. As regiões $R(s,v)$ são invariantes por esta rotação: na verdade, são claramente invariantes sob o grupo de isometrias do reticulado $\mathbb{Z}^2$ com a métrica do grafo (que é a métrica da soma dos módulos). Este grupo, que foi calculado em [30, 28], contém o grupo gerado pelas reflexões nos eixos coordenados e nas bissetrizes e é isomorfo ao grupo diedral de oito elementos, $\mathbb{D}_4$. A ação de $\mathbb{D}_4$ nas regiões é dada por $g(R(s,v)) = R(s,gv)$. Logo, o ladrilhamento do plano por Λ_1 com região fundamental $R(s,0)$ é levado em um ladrilhamento do plano por $g(\Lambda_1) = \Lambda_2$ com região fundamental $R(s,0)$.

Seja agora Λ um reticulado que ladrilha o plano com a região $R(s,0)$. Vamos estudar Λ pelos vetores que emparelham regiões com $R(s,0)$, isto é, pelos vetores $v\in\Lambda$ tais que $R(s,0)$ e $R(s,v)$ têm intersecção ao longo de lados de quadrados[2]. Como as regiões referidas são uniões de quadrados centrados nos pontos de $\mathbb{Z}^2$, esta intersecção tem que ser ao longo de lados de quadrados. A outra possibilidade é intersecção em vértices de quadrados apenas, mas neste caso não há ladrilhamento algum.

Mostraremos então que, se v é tal que $R(s,v)$ e $R(s,0)$ estão pareadas, então $||v|| = 2s+1$.

Sem perda de generalidade, considere um vetor v com coordenadas inteiras não-negativas e suponha que $||v||\leq 2s$. Se $v_2 \leq \left\lfloor\frac{||v||}{2}\right\rfloor$, tome o vetor $w = \left(v_1 - \left\lfloor\frac{||v||}{2}\right\rfloor, v_2\right)$. Temos que $||w|| = v_1 - \left\lfloor\frac{||v||}{2}\right\rfloor + v_2 = ||v|| - \left\lfloor\frac{||v||}{2}\right\rfloor \leq s$, e $||w-v|| = \left\lfloor\frac{||v||}{2}\right\rfloor \leq s$. Logo, o quadrado unitário centrado em w está contido em $R(s,0)$ e $R(s,v)$, de modo que o vetor v não pode

[2]Como as regiões referidas são uniões de quadrados centrados nos pontos de $\mathbb{Z}^2$,, esta intersecção tem que ser ao longo de lados de quadrados ou em vértices apenas.

pertencer a Λ. Se $\left\lfloor \frac{||v||}{2} \right\rfloor < v_2 \leq ||v||$, tome o vetor $w' = \left(v_1, v_2 - \left\lfloor \frac{||v||}{2} \right\rfloor\right)$. As mesmas contas mostram que $R(s,0)$ e $R(s,v)$ têm um quadrado em comum. Portanto, qualquer vetor de Λ possui norma maior do que (ou igual a) $2s+1$.

Agora suponha que $R(s,0)$ e $R(s,v)$ são pareadas por $v \in \Lambda$. Para que isto ocorra é necessário que ao menos um lado de um quadrado de $R(s,0)$ coincida com um lado de um de $R(s,v)$. Isto acontece apenas se existirem dois vetores $w, w' \in \mathbb{Z}^2$ tais que $||w - w'|| = 1$, $||w|| \leq n$, $||w' - v|| \leq n$. Então $||v|| \leq ||v - w'|| + ||w - w'|| + ||w|| \leq 2s+1$. Pelo visto no parágrafo anterior, concluímos que $||v|| = 2s+1$. Isto também mostra que a norma mínima de um vetor de Λ é $2s+1$ (não confundir com a norma mínima *euclidiana*, que assume outros valores em Λ).

Suponha que v é da forma $v = (s+k, s+1-k)$, com $k \geq 0$. Queremos mostrar que $k = 0$ ou 1. Para isso, vamos considerar um ponto extremo de $R(s,v)$, o vetor $v-(s,0) = (k, s+1-k)$, e três pontos vizinhos: $v - (s+1,0) = (k-1, s+1-k)$, $v - (s,-1) = (k, s+2-k)$ e $v-(s+1,-1) = (k-1, s+2-k)$. O ponto $v-(s+1,0)$ está contido em $R(s,0)$, e os pontos restantes estão em outros dois poliedros do ladrilhamento. Vamos mostrar que se $k > 1$ então estes dois poliedros se interceptam (e portanto não existe rotulamento possível).

Suponha que $k > 1$. Seja $R(s,w_1)$ a região que contém o ponto $v-(s,-1) = (k, s+2-k)$. Afirmamos que $w_1 = (k, s+2)$. De fato, o quadrado $Q((k, s+2-k))$ está acima do quadrado $Q((k, s+1-k))$, que está contido em $R(s,0)$; e está à esquerda do quadrado $Q((k, s+1-k))$, que está contido em $R(s,v)$. Pela geometria destas regiões, o quadrado $Q((k, s+2-k))$ é o extremo inferior de $R(s,w_1)$. Logo, w_1 é o vetor $(k, s+2)$.

Por raciocínio análogo, a região que contém com o ponto $(k-1, s+2-k)$ mostra que a região que contém o quadrado $Q((k-1, s+2-k))$ é $R(s,w_2)$ com $w_2 = (k-1, s+2)$. Portanto, as regiões $R(s,w_1)$ e $R(s,w_2)$ se interceptam em ao menos um quadrado, e não pode haver ladrilhamento. Logo, $k = 0$ ou 1.

O caso $v = (l, 2s+1-l)$, $0 \leq l < s$, não se realiza. De fato, suponha que existe um ladrilhamento por um reticulado Λ', com região $R(s,0)$ e tal que $v = (l, 2s+1-l) \in \Lambda'$, $0 \leq l < s$. Aplicando a reflexão $T(x,y) = (y,x)$ obtemos um ladrilhamento pelo reticulado $T\Lambda'$ que possui o vetor $(2s+1-l, l)$, cuja primeira coordenada é maior do que $s+1$, o que não pode ocorrer. Deste modo, dentre os vetores $(k, 2s+1-k)$ com k positivo, apenas $(s, s+1)$ e $(s+1, s)$ podem pertencer a Λ.

Aplicando as reflexões em eixos coordenados podemos investigar outros possíveis vetores mínimos de Λ reduzindo ao caso $v = (k, 2s+1-k)$, $0 \leq k \leq 2s+1$. Assim concluímos que os únicos pontos de norma $2s+1$ que podem estar em Λ são $(\pm(s+1), \pm s)$ e $(\pm s, \pm(s+1))$.

Para finalmente determinar Λ, suponha que $(s, s+1)$ pertence a este reticulado. Necessariamente um dos pontos $(-s-1, s)$ e $(-s, s+1)$ também pertence a ele. Os vetores $(s, s+1)$ e $(-s, s+1)$ não podem estar ambos em Λ, pois sua diferença é $(2s, 0)$, e a norma mínima em Λ é $2s+1$. Neste caso $\Lambda = \langle\{(s, s+1), (-s-1, s)\}\rangle = \Lambda_1$. Do mesmo modo, se $(s+1, s)$ pertence a Λ, o vetor $(-s-1, s)$ não pertence a Λ, e $\Lambda = \Lambda_2$. ■

Como consequência, podemos agora descrever todos os códigos lineares perfeitos em dimensão 2.

Teorema 9 *Dados n e m positivos, existem dois códigos lineares perfeitos em $\left(\mathbb{Z}_q^2, d_l\right)$, onde $q = m\left(2n^2+2n+1\right)$. Estes códigos são equivalentes.*

Demonstração. Pelo teorema 4, o código perfeito C corresponde a um ladrilhamento de $\mathbb{R}^2$ por um reticulado. Vimos que os únicos reticulados que ladrilham o plano com a região $R(n,0)$ que corresponde à bola de Lee de raio n são Λ_1 e Λ_2.

Pelos teoremas 3 e 5, o ladrilhamento por Λ_i induz outro no toro $\mathbb{R}^2/\Lambda$ se, e somente se, $\Lambda < \Lambda_i$. No caso de espaços de Lee, $\Lambda = q\mathbb{Z}^2$. Em ambos os reticulados Λ_i temos $q\mathbb{Z}^2 < \Lambda_i$ se e só se $q = m\left(2n^2+2n+1\right)$. Para ver isso, oberve que $(q,0)$ pertence a Λ_1 se e só se

$$\begin{bmatrix} n+1 & -n \\ n & n+1 \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} = \begin{bmatrix} q \\ 0 \end{bmatrix}$$

para x e y inteiros. Invertendo a matriz, obtemos

$$(x,y) = q\left(\frac{n+1}{2n^2+2n+1}, -\frac{n}{2n^2+2n+1}\right) \in \mathbb{Z}^2,$$

e como n não divide $2n^2+2n+1$, segue que $q = m\left(2n^2+2n+1\right)$. A verificação para Λ_2 é análoga[3]. Assim, concluímos que os ladrilhamentos por Λ_1 e Λ_2 descem aos espaços de Lee $\left(\mathbb{Z}^2_{m(2n^2+2n+1)}, d_l\right)$.

Os códigos obtidos são quocientes de reticulados, e portanto são lineares sobre $\mathbb{Z}^2_{m(2n^2+2n+1)}$, ou seja, são retas. Para encontrá-las, considere primeiro $m=1$, e seja v um ponto de Λ_1. Então $v = x(n,n+1) + y(-n-1,n) = (nx-ny-y, nx+n+ny)$. Este ponto satisfaz

$$\begin{aligned} (2n+1)v_1 + v_2 &= \left(2n^2+2n+1\right)x + \left(2n^2+2n+1\right)y \\ &= 0 \bmod \left(2n^2+2n+1\right) \end{aligned}$$

Portanto, a imagem de Λ_1 é a reta $(2n+1)v_1 + v_2 = 0$, ou ainda $v(t) = (-t, (2n+1)t)$. Para Λ_2 obtemos a reta $(2n+1)v_1 - v_2 = 0$.

No caso geral, com $q = m\left(2n^2+2n+1\right)$, as retas são[4]

$$\begin{aligned} m(2n+1)v_1 + mv_2 &= 0, \\ m(2n+1)v_1 - mv_2 &= 0. \end{aligned}$$

Estes códigos são equivalentes: a reflexão $(x,y) \mapsto (y,x)$ é uma isometria linear que leva um código no outro. ■

[3] n divide $2n^2+2n$, e por isso não pode dividir $(2n^2+2n)+1$, senão dividiria 1.

[4] estas retas não são as mesmas retas anteriores; note que m não é invertível em $\mathbb{Z}_{m\left(2n^2+2n+1\right)}$, e não podemos cancelar m.

2.5 Rotulamentos não-abelianos em Espaços de Lee

A construção de rotulamentos de espaços ambientes é motivada pelos códigos quaternários em espaços de Hamming. O rotulamento de $\left(\mathbb{Z}_2^{2n}, d_h\right)$ por um grupo de rotações isomorfo a $(\mathbb{Z}_4^n, +)$ permite estudar códigos não-lineares binários como códigos lineares em $\mathbb{Z}_4^n$. Como códigos lineares são $\mathbb{Z}_4$-submódulos de $\mathbb{Z}_4^n$, e estes submódulos são simplesmente subgrupos de $(\mathbb{Z}_4^n, +)$, uma extensão natural deste conceito é tomar grupos rotuladores gerais e aplicar os mesmos processos: considerar os códigos dados por subgrupos de um grupo rotulador. Esta é a idéia por trás da G-linearidade [19, 13], que será discutida com detalhes no próximo capítulo.

Rotulamentos cíclicos seriam desejáveis, seja por conta da simplicidade dos grupos envolvidos, seja pelas técnicas disponíveis para construção de códigos sobre anéis do tipo $\mathbb{Z}_{p^n}$, p primo. Mas o único rotulamento deste tipo é o de $\mathbb{Z}_2^2$ por $\mathbb{Z}_4$, como mostramos em [13]. Tampouco existem parametrizações por grupos abelianos distintos dos grupos de translação [30, 28]. Portanto, se houvesse algum rotulamento além do usual, este teria que ser feito por um grupo não-comutativo, e é isso que motiva o exemplo que será construído a seguir.

Nesta seção apresentamos parametrizações para uma família de espaços de Lee, os espaços $(\mathbb{Z}_{2m}^n, d_l)$, via ladrilhamentos de $\mathbb{R}^n$. Estas construções fazem parte do artigo [28].

Os rotulamentos para $(\mathbb{Z}_{2m}^n, d_{lee})$ são construídos a partir de parametrizações do reticulado $\mathbb{Z}^n$. Para manter a notação simples, usaremos o reticulado deslocado $\Lambda^n = \mathbb{Z}^n + \sum \frac{1}{2} e_i$. Faremos os mesmo sobre os toros, onde vamos considerar o reticulado quociente $\Lambda_{2m}^n = \Lambda^n / 2m\mathbb{Z}$ sobre o toro $T_{2m}^n = \mathbb{R}^n / 2m\mathbb{Z}$. No fim, para obter um rotulamento do espaço de Lee propriamente, basta conjugar o grupo parametrizador por uma translação que leve Λ_{2m}^n em $\mathbb{Z}_{2m}^n$.

O grupo é construído a partir de dois grupos de isometrias. O primeiro age nos vértices do cubo $[-1/2, 1/2]^n$, e o segundo é um grupo de translações que preserva Λ^n e que tem o cubo "duplo" $[-1/2, 3/2]^n$ como região fundamental. O grupo gerado por esses dois grupos, que terá a estrutura de um produto semi-direto, será o grupo rotulador de Λ^n. Passando ao quociente, obteremos rotulamentos de Λ_{2m}^n. A razão para utilizar Λ^n ao invés de $\mathbb{Z}^n$ é que o "grupo interno" que rotula o cubo unitário $[-1/2, 1/2]^n$ pode ser escrito como um grupo de matrizes (o que seria impossível se trabalhássemos com $[0, 1]^n$ em $\mathbb{Z}^n$).

Para entender a idéia, façamos primeiro um exemplo bidimensional. Considere o grupo $\mathbb{D}$ das reflexões nos eixos coordenados. Este grupo parametriza o quadrado $[-1/2, 1/2]^2$, e a extensão disto a um rotulamento de Λ^2 pode ser feita por translações do quadrado de lado dois $[-1/2, 3/2]^2$: o plano é coberto pelos transladados deste quadrado, e cada ponto de Λ^2 está em um único quadrado $[-1/2, 1/2]^2 + v$, com $v \in 2\mathbb{Z}^2$. Podemos então usar a parametrização em $[-1/2, 1/2]^2$ e dar novas coordenadas a estes pontos: cada ponto de Λ^2 fica descrito por um elemento de $\mathbb{D}$ e por uma translação do tipo $(2k_1, 2k_2)$, k_1, k_2 inteiros. O grupo gerado pelo grupo de reflexões $\mathbb{D}$ e pelo reticulado $2\mathbb{Z}^2$ é o produto semi-direto destes, e as aquelas novas coordenadas correspondem ao rotulamento de Λ^2 por $2\mathbb{Z}^2 \rtimes \mathbb{D}$. Finalmente, como o grupo de translações $2m\mathbb{Z}^2$ é normal neste grupo, obtemos o rotulamento de Λ_{2m}^2 por $\left(2\mathbb{Z}^2 \rtimes \mathbb{D}\right) / 2m\mathbb{Z}^2$, que é isomorfo a $\mathbb{Z}_2^2 \ltimes \mathbb{Z}_m^2$.

Para estender isto a outras dimensões, no lugar de $\mathbb{D}$ vamos considerar o grupo gerado por reflexões em hiperplanos coordenados, e como grupo de translações tomaremos o reticulado $2\mathbb{Z}^n$. Estes grupos geram o grupo $\mathbb{G} = \{T = \tau_u A; : A = diag(\pm 1, ..., \pm 1), : u \in 2\mathbb{Z}^n\}$ que fará o rotulamento.

Teorema 10 *Seja $\mathbb{G}$ o grupo de simetrias gerado pelas reflexões em hiperplanos coordenados e por translações por elementos de $2\mathbb{Z}^n$.*

(i) $\mathbb{G}$ é isomorfo a $\mathbb{Z}^n \rtimes \mathbb{Z}_2^n$

(ii) O cubo $[-1/2, 3/2]^n$ é uma região fundamental para a ação de $2\mathbb{Z}^n$.

(iii) O grupo $\mathbb{G}$ age livre e transitivamente em Λ^n. Se $g = \tau_u A$, $supp(A)$ é o conjunto $supp(A) = \{i; a_{ii} = -1\}$ (o suporte de A), e $supp(\tau_u) = \{i; u_i \neq 0\}$, então o conjunto de pontos fixos de g é

$$F(g) = \left\{ \sum_{\substack{i \notin supp(A) \\ i \notin supp(\tau_u)}} c_i e_i + \sum_{i \in supp(A)} \frac{1}{2} u_i e_i ; c_i \in \mathbb{R} \right\}.$$

(iv) $\mathbb{G}$ induz um grupo de simetrias $\mathbb{G}_{2m}^n$ no toro $T_{2m}^n = \mathbb{R}^n / 2\mathbb{Z}^m$ que também age livre e transitivamente nos reticulados quocientes $\Lambda_{2m}^n = \Lambda^n / 2m\mathbb{Z}^n$. Portanto, $\mathbb{G}_{2m}^n$ define um rotulamento do espaço de Lee $(\mathbb{Z}_{2m}^n, d_{lee})$. O grupo $\mathbb{G}_{2m}^n$ é isomorfo a $\mathbb{Z}_m^n \rtimes \mathbb{Z}_2^n$.

Demonstração. (i) O produto semi-direto $\mathbb{Z}^n \rtimes \mathbb{Z}_2^n$ a que nos referimos vem da ação canônica de $\mathbb{Z}_2^n$ como grupo de automorfismos de $\mathbb{Z}^n$: para $\sigma = (a_1, ..., a_n) \in \mathbb{Z}_2^n$ e um vetor $v \in \mathbb{Z}^n$, $\sigma(v) = ((-1)^{a_1} v_1, ..., (-1)^{a_n} v_n)$. O grupo de matrizes diagonais $\mathbb{D} = diag(\pm 1, \ldots, \pm 1)$ e o grupo $\mathbb{Z}_2^n$ são isomorfos via

$$\begin{array}{rccc} \theta: & \mathbb{D} & \longrightarrow & \mathbb{Z}_2^n \\ & A & \longmapsto & (\delta(a_{11}), \ldots, \delta(a_{nn})) \end{array}$$

onde $\delta(-1) = 1$ e $\delta(1) = 0$. A aplicação

$$\begin{array}{rccc} \phi: & \mathbb{G} & \longrightarrow & \mathbb{Z}^n \rtimes \mathbb{Z}_2^n \\ & \tau_u A & \longmapsto & (1/2u, \theta(A)) \end{array}$$

é um isomorfismo entre $\mathbb{G}$ e $\mathbb{Z}^n \rtimes \mathbb{Z}_2^n$.

(ii) Para facilitar as contas, mostraremos que $R = [0, 2]^n$ é região fundamental para $2\mathbb{Z}^n$. Como a imagem por isometria de uma região fundamental também é uma região fundamental, e $[-1/2, 3/2]^n = -\sum \frac{1}{2} e_i + R$, isto basta para demonstrar (ii). Seja $v \in int(R)$, e suponha que $\tau_u v \in int(R)$, para algum $u \in 2\mathbb{Z}^n$. Isto é, $\sum (u_i + v_i) e_i \in int(R)$, ou ainda, $0 < u_i + v_i < 2$, para todo i. Por hipótese, $u_i = 2k_i$, $k_i \in \mathbb{Z}$, e $0 < v_i < 2$. Logo, se $u_i \neq 0$, $u_i + v_i$ não pertence a $(0, 2)$, e $\tau_u v$ não pertence a $int(R)$. Isto mostra que $int(R) \cap \tau_u int(R) = \varnothing$ (ou ainda, $int(R) \cap int(\tau_u R) = \varnothing$, pois $int(\tau_u R) = \tau_u int(R)$).

Além disso, $\mathbb{R}^n = \bigcup_{u \in 2\mathbb{Z}^n} \tau_u(R)$. Basta ver que cada vetor v de $\mathbb{R}^n$ pode ser escrito como $v = \sum 2 \lfloor v_i/2 \rfloor e_i + \sum (v_i - 2 \lfloor v_i/2 \rfloor) e_i$, em que o primeiro termo está em $2\mathbb{Z}^n$ e o segundo em $\mathbb{R}$. Portanto, R é região fundamental para $2\mathbb{Z}^n$.

(iii) Para demonstrar que a ação é transitiva em Λ^n, vamos mostrar que Λ^n é a órbita de $-\sum \frac{1}{2}e_i$ sob $\mathbb{G}$. Primeiro, considere um ponto v de Λ^n contido em $[-1/2, 3/2]^n$. Para um conjunto de índices $I \subset S = \{1, 2, ..., n\}$, seja σ_i a reflexão $(v_1, .., v_i, ..., v_n) \mapsto (v_1, .., -v_i, ..., v_n)$, e seja σ_I a isometria $\sigma_I = \prod_{i \in I} \sigma_i$. Se $v = \sum_{i \in I} \frac{1}{2}e_i - \sum_{j \in S \setminus I} \frac{1}{2}e_j$, então claramente $v = \sigma_I\left(-\sum \frac{1}{2}e_i\right)$. Isto resolve tudo, pois os outros pontos v em $\Lambda^n \cap [-1/2, 3/2]^n$ podem ser trazidos para $[-1/2, 1/2]^n$ por uma translação apropriada de um elemento de $2\mathbb{Z}^n$; logo, todos os pontos de $\Lambda^n \cap [-1/2, 3/2]^n$ estão na órbita de $-\sum \frac{1}{2}e_i$. Como $[-1/2, 3/2]^n$ é uma região fundamental para $2\mathbb{Z}^n$, para qualquer ponto v de Λ^n existe $\tau_u \in 2\mathbb{Z}^n$ tal que $\tau_u(v)$ pertence a $\Lambda^n \cap [-1/2, 3/2]^n$, e por conseguinte, à órbita de $-\sum \frac{1}{2}e_i$. Isto mostra que $\mathbb{G}$ age transitivamente.

Por tabela, sabemos que os estabilizadores $\mathbb{G}_p = \{g \in \mathbb{G}; g(p) = p\}$ são conjugados. Logo, basta mostrar que um deles é trivial para concluir que a ação é livre. Para estas contas vamos tomar o ponto $p = \sum \frac{1}{2}e_i$.

Primeiro, descrevamos o conjunto de pontos fixos de um elemento de $\mathbb{G}$. Seja $g = \tau_u A$ e suponha que v é fixado por g. Temos as equações

$$(a_{ii} - 1)v_i + u_i = 0, \qquad i = 1, ..., n.$$

Para cada i, ou ocorre $a_{ii} = 1$, e então $u_i = 0$, e v_i é um número arbitrário, ou $a_{ii} = -1$, e necessariamente $v_i = \frac{1}{2}u_i$. Sendo $supp(A) = \{i; a_{ii} = -1\}$, podemos descrever o conjunto de pontos fixos de g como $F(g) = \left\{ \sum_{\substack{i \notin supp(A) \\ i \notin supp(\tau_u)}} a_i e_i + \sum_{i \in supp(A)} \frac{1}{2}u_i e_i; a_i \in \mathbb{R} \right\}$.

Voltando ao ponto $p = \sum \frac{1}{2}e_i$: este ponto não está em nenhum $F(g)$. De fato, já que $u \in 2\mathbb{Z}^n$, $p = \sum \frac{1}{2}e_i$ não pertence a nenhum $F(\tau_u A)$ se $supp(A) \neq \emptyset$, e $supp(A) = \emptyset$ se e só se g é uma translação pura, $g = \tau_u$. Logo, g fixa o ponto $\sum \frac{1}{2}e_i$ se e só se $g = id$.

(iv) Para conseguir o rotulamento dos reticulados Λ^n_{2m}, usamos a projeção canônica no toro $T^n_{2m} = \mathbb{R}^n/2m\mathbb{Z}^n$ para induzir uma ação do grupo quociente $\mathbb{G}^n_{2m} = \mathbb{G}/2m\mathbb{Z}^n$. Usando a isometria $v \mapsto v - \sum \frac{1}{2}e_i$ de T^n_{2m} obtemos o rotulamento do espaço de Lee correspondente.

Para começar, observamos que $2m\mathbb{Z}^n$ é um subgrupo normal de $\mathbb{G}$; isto segue das contas feitas no item (i). Logo, pelo teorema 3, $\mathbb{G}^n_{2m} = \mathbb{G}/2m\mathbb{Z}^n$ é um grupo de simetrias de T^n_{2m}. O subgrupo de transformações lineares $\mathbb{D}$ não é afetado pelo quociente, isto é, cada aplicação A está em uma classe lateral distinta. Mais especificamente, podemos considerar a seguinte aplicação, que é composta de ϕ com a projeção $\mathbb{Z}^n \to \mathbb{Z}^n_m$:

$$\begin{array}{rccc} \phi_m : & \mathbb{G} & \longrightarrow & \mathbb{Z}^n_m \rtimes \mathbb{Z}^n_2 \\ & \tau_u A & \longmapsto & (1/2u + m\mathbb{Z}^n, \theta(A)) \end{array}$$

Esta ϕ_m é sobre, e seu núcleo é o grupo de translações $2m\mathbb{Z}^n$. Portanto, temos um isomorfismo entre $\mathbb{G}^n_{2m}$ e $\mathbb{Z}^n_m \rtimes \mathbb{Z}^n_2$.

Continuando: a ação de $\mathbb{G}^n_{2m}$ em $\Lambda^n_{2m} = \Lambda^n/2m\mathbb{Z}^n$ é obviamente transitiva, pois a de $\mathbb{G}$ é transitiva em Λ^n. Para verificar que a ação é livre devemos examinar as mesmas equações de pontos fixos:

$$(a_{ii} - 1)v_i + u_i = 0 \bmod 2m, \qquad i = 1, ..., n.$$

Ao invés de descrever o conjunto dos pontos fixos, vamos mostrar diretamente que $\sum \frac{1}{2}e_i$ não pode ser fixado por um elemento diferente da identidade. Suponha que g fixa o ponto $\sum \frac{1}{2}e_i$. Se $a_{ii} = -1$, $u_i = 2v_i \bmod 2m$. Para $v_i = 1/2$ nós obtemos $u_i = 1 \bmod 2m$, impossível, pois $u_i \in 2\mathbb{Z}_m$. Então todo $a_i = 1$ e $u_i = 0 \bmod 2m$, i.e., $g = id$. Isto termina a demonstração. ■

Com pequenas alterações, esta demonstração também serve para um outro ladrilhamento, desta vez apenas bidimensional.

Exemplo 6 *Um ladrilhamento de $\mathbb{Z}^2_{4m}$ — no caso bidimensional podemos também considerar um ladrilhamento que segue um padrão alternado, como o da colocação de tijolos em um muro. Nós tomamos o grupo $\mathbb{H} = \{\tau_u A; u \in L,\ A = diag(\pm 1, \pm 1)\}$ onde L é o reticulado $L = \{a(2,1) + b(2,-1);\ a, b \in \mathbb{Z}\}$. O grupo rotulador é $\mathbb{H} = \{\tau_u A; u \in L,\ A = diag(\pm 1, \pm 1)\}$. O reticulado $4m\mathbb{Z}^2$ é um subgrupo normal de $\mathbb{H}$, e por isso obtemos um ladrilhamento do toro T^2_{4m} pelo grupo $\mathbb{H}_{4m} = \{\tau_u A; u \in L/4m\mathbb{Z}^2,\ A = diag(\pm 1, \pm 1)\}$, o que fornece um rotulamento de L^2_{4m}.*

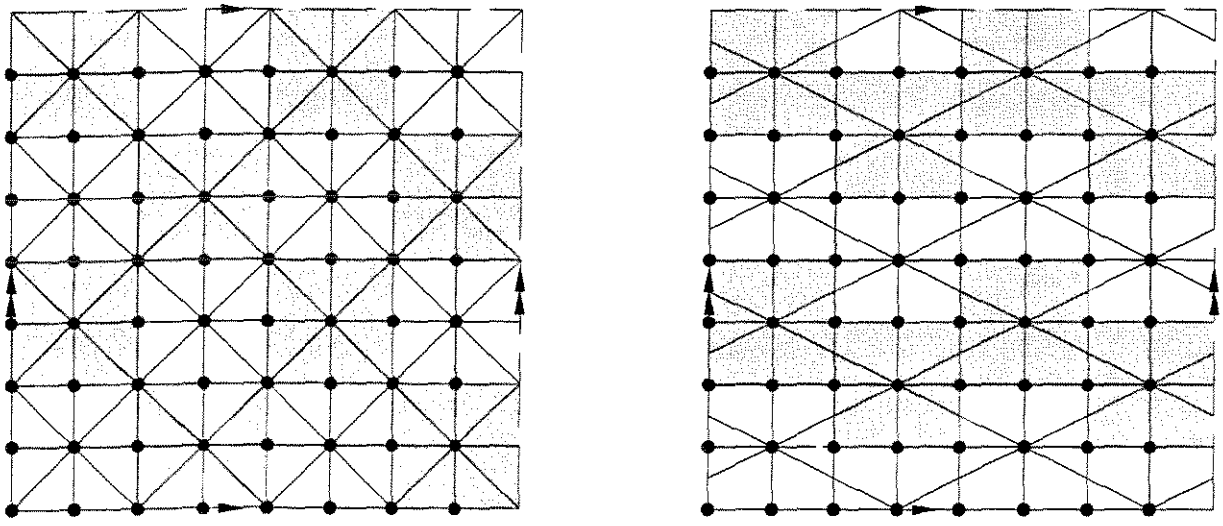


FIGURA 2 Ladrilhamentos de $(\mathbb{Z}^2_8, d_l)$.

Capítulo 3

Códigos Propelineares e G-lineares binários

3.1 Introdução

Neste capítulo e no próximo nós trataremos de códigos em espaços de Hamming e rotulamentos. O assunto deste capítulo é a relação existente entre duas maneiras de trabalhar com rotulamentos de códigos em $\mathbb{Z}_2^n$. Os códigos propelineares do título foram primeiro apresentados em [37] como generalizações de pré-imagens de recobrimentos de grafos pelo grafo de Hamming, isto é, do n-cubo. Os códigos são primeiramente tomados como pré-imagens da projeção da origem. Ou seja, se $\theta : (\mathbb{Z}_2^n, d) \to \Gamma$ é o recobrimento, o código $\mathcal{C}$ é $\theta^{-1}(\theta(0))$. Sob certas condições é possível associar um grupo de permutações de coordenadas a este código. A generalização disto é considerar códigos $\mathcal{C} \subset (\mathbb{Z}_2^n, d)$ e aplicações injetoras destes no grupo de permutações de coordenadas satisfazendo as mesmas condições do caso anterior, onde $\mathcal{C}$ é pré-imagem de um recobrimento. Este grupo é utilizado pra fornecer uma estrutura algébrica a $\mathcal{C}$, chamada estrutura propelinear do código em [37].

Paralelamente, temos outro conceito que também utiliza grupos de permutações, pois é baseado em grupos de simetrias. Os códigos G-lineares, apresentados em [19, 13], são construídos via rotulamentos do espaço ambiente. Quando o espaço é o binário, os grupos rotuladores são subgrupos de $\mathbb{Z}_2^n \rtimes S_n$. Aparentemente, estas são duas maneiras bem distintas de fornecer estrutura de grupo a códigos não-lineares. Na verdade, a estrutura propelinear nada mais é do que um subgrupo N de $\mathbb{Z}_2^n \rtimes S_n$ que age livremente em sua órbita $N(0)$. Este é um dos principais resultados desta parte (teorema 11).

Ambos os conceitos incluem os códigos quaternários (e os propelineares são anteriores a estes). Somas de códigos binários e quaternários são a classe mais importante de códigos propelineares em termos de aplicações a códigos perfeitos [6]; são os códigos propelineares (abelianos) invariantes por translação. Entre esta classe e a de todos os propelineares estão os G-lineares. Neste capítulo nós fornecemos uma descrição dos códigos propelineares em termos de grupos de simetrias e mostramos as relações entre estes e os códigos G-lineares binários. Ao final, estu-

damos a extensão da subclasse dos códigos propelineares invariantes por translação para outros alfabetos.

Esta parte da tese consiste basicamente de resultados publicados em [31], trabalho realizado com Sueli Costa, João Gerônimo, Reginaldo Palazzo Jr., J.C. Interlando e Martinho Araújo. Fornecemos aqui novos exemplos de códigos propelineares, e a seção sobre propelineares em outros espaços de Hamming estende um resultado provado em [2] (ver também [3]).

3.2 Códigos Propelineares

Códigos propelineares foram definidos originalmente em [37] com o intuito de estudar relações entre códigos e grafos, em especial códigos perfeitos.

Neste capítulo d denotará a distância de Hamming, salvo menção em contrário.

Definição 19 *[37] Seja Γ um grafo conexo. Uma aplicação $\theta : (\mathbb{Z}_2^n, d) \to \Gamma$ é um r-isomorfismo local se, para cada u de $\mathbb{Z}_2^n$ e $0 < s < r$, a restrição de θ à bola $B_s(u)$ é uma isometria.*

Associado a esta aplicação está o código binário $\mathrm{C}(0) = \{u \in \mathbb{Z}_2^n; \theta(u) = \theta(0)\}$. No mesmo artigo é provado que, se $r \geq 3$, e $\theta(a) = \theta(b)$, então existe uma permutação de coordenadas π_{ab} tal que $\theta(a + s) = \theta(b + \pi_{ab}(s))$. Fazendo $a = 0$ e $b = v$, com $\theta(v) = \theta(0)$, obtemos uma aplicação injetora π :C(0) $\to S_n$ dada por $v \longmapsto \pi_v$, onde π_v é a única permutação tal que $\theta(s) = \theta(v + \pi_v(s))$ para todo s em $\mathbb{Z}_2^n$. Isto sugere a definição de propelinearidade: uma estrutura propelinear para um código C é uma função que associa a cada palavra v de C uma permutação de coordenadas π_v de modo que o código seja invariante sob a isometria $\tau_v\pi_v$ (onde τ_v é a translação pelo vetor v). É importante ter em mente que o mesmo código pode ter várias estruturas propelineares, do mesmo modo que pode ter vários rotulamentos distintos.

A conexão com códigos quaternários se dá por dois motivos: primeiramente, todo $\mathbb{Z}_4$-linear é propelinear; além disso, a principal aplicação a códigos perfeitos envolve códigos que são soma direta de lineares e $\mathbb{Z}_4$-lineares [6]. Finalmente, como demonstrado em [37], as únicas estruturas propelineares abelianas são dadas por grupos do tipo $\mathbb{Z}_2^{n_1} \times \mathbb{Z}_4^{n_2}$. Ou seja, códigos propelineares abelianos são somas diretas de lineares e quaternários.

Definição 20 *[37] Seja C um código de $\mathbb{Z}_2^n$ que contém o vetor nulo. Dizemos que este código é propelinear se existir um conjunto de permutações de coordenadas $\Pi = \{\pi_v \mid v \in C\}$ tal que*

(1) Para cada $v \in C$, $v + \pi_v(s) \in C$ se e só se $s \in C$;

(2) Para cada par π_u, $\pi_v \in \Pi$, o produto $\pi_u\pi_v$ é a permutação π_w (que pertence a Π) onde $w = u + \pi_u(v)$.

A relação desta definição com o código $\mathcal{C}(0)$ associado a um r-isomorfismo local é dada no mesmo artigo: a aplicação $\pi : \mathcal{C}(0) \to S_n$ satisfaz (1) e (2) da definição acima. Mostra-se que Π é um grupo, e que o próprio código propelinear tem uma estrutura de grupo induzida por π. As operações são

$$\begin{aligned} uv &= u + \pi_u(v) \\ u^{-1} &= -\pi_u^{-1}(u) \end{aligned}$$

Usando (1) e (2) da definição 20 e o fato de Π ser grupo pode-se verificar que as operações acima tornam C um grupo. Mas isto pode ser visto de modo mais simples, usando uma caracterização destes códigos em termos de grupos de simetrias.

3.2.1 O grupo de simetrias do espaço de Hamming binário

Como foi visto no capítulo 1, as isometrias de $(\mathbb{Z}_2^n, d)$ possuem uma decomposição natural: toda isometria f se escreve de modo único como um produto $f = \sigma\pi$, onde π é uma permutação de coordenadas, e σ é um produto de permutações de elementos do alfabeto feitas coordenada a coordenada, $\sigma = (\sigma_1, \ldots, \sigma_n)$. Como cada σ_i é uma permutação do alfabeto $\mathbb{Z}_2$, na verdade a aplicação σ é uma translação τ_u, e temos o isomorfismo

$$\begin{array}{ccc} \mathbb{S}(\mathbb{Z}_2^n, d) & \to & \mathbb{Z}_2^n \rtimes S(n) \\ \tau_u\pi & \longmapsto & (u, \pi) \end{array}$$

O produto semi-direto considerado é dado por

$$(u, \pi)\,(v, \sigma) = (u + \pi(v), \pi\sigma)$$

o que corresponde à ação do subgrupo de permutações nas translações de $\mathbb{Z}_2^n$. No que segue, identificaremos $\mathbb{S}(\mathbb{Z}_2^n, d)$ e $\mathbb{Z}_2^n \rtimes S_n$ (por meio do isomorfismo acima).

A estrutura propelinear é induzida do grupo de simetrias do espaço de Hamming. Começamos por observar que estes códigos são definidos por uma aplicação $\pi : C \to S_n$, $\pi(v) = \pi_v$, cujo grafo $\Omega(\pi) = \{(v, \pi_v) | v \in C\}$ pode ser identificado com um subconjunto do grupo $\mathbb{S}(\mathbb{Z}_2^n, d)$. Na verdade, é um subgrupo deste.

Lema 4 *Seja $(\mathbb{Z}_2^n, d)$ o espaço de Hamming de dimensão n sobre $\mathbb{Z}_2$, e seja S_n o grupo simétrico de grau n. Um código $C \subseteq \mathbb{Z}_2^n$ que contém o vetor nulo é* ***propelinear*** *se e só se existir uma função*

$$\begin{array}{rcl} \pi : C & \to & S_n \\ v & \longmapsto & \pi_v \end{array}$$

tal que seu grafo

$$\Omega(\pi) = \{(v, \pi_v)\,|\, v \in C\},$$

seja um subgrupo do grupo de simetrias de $(\mathbb{Z}_2^n, d)$.

Demonstração. Seja $\mathcal{C}$ um código propelinear, e considere o grafo $\Omega(\pi)$ da aplicação π de C em S_n. Para (v, π_v) e (u, π_u) em $\Omega(\pi)$, temos

$$(v, \pi_v)(u, \pi_u) = (v + \pi_v(u), \pi_v\pi_u) = (v + \pi_v(u), \pi_{v+\pi_v(u)}),$$

pelo item (2) da Definição 20. Como $u \in C$, segue que $v + \pi_v(u) \in C$ ((1) da Definição 20), e portanto $\Omega(\pi)$ é fechado sob multiplicação. Como Π é subgrupo de S_n, $\pi_u^{-1} \in \Pi$. Além disso, $C \ni 0 = u + \pi_u\left(-\pi_u^{-1}(u)\right)$, e $-\pi_u^{-1}(u) \in C$ pelo item (1) da Definição 20. Como $(u, \pi_u)^{-1} = (-\pi_u^{-1}(u), \pi_u^{-1})$, $(u, \pi_u)^{-1} \in \Omega(\pi)$.

Para a volta, suponha que $\mathcal{C}$ é um código e $\pi : \mathcal{C} \to S_n$ é uma aplicação tal que $\Omega(\pi) = \{(v, \pi_v) \,|\forall v \in \mathcal{C}\}$ é subgrupo de $\mathbb{Z}_2^n \rtimes S_n$. Claramente, vale (2) da definição de código propelinear, pois $(v, \pi_v)(u, \pi_u) = (v + \pi_v(u), \pi_v\pi_u)$ e $\Omega(\pi)$ é subgrupo, o que implica em $\pi_v\pi_u = \pi_{v+\pi_v(u)}$.

Quanto ao primeiro item, sejam $v \in \mathcal{C}$ e $s \in \mathbb{Z}_2^n$ tais que $w = v + \pi_v(s) \in \mathcal{C}$, e seja (w, π_w) o elemento correspondente em $\Omega(\pi)$. Como $(-\pi_v^{-1}(v), \pi_v^{-1}) = (v, \pi_v)^{-1}$ pertence a $\Omega(\pi)$, $s = \pi_v^{-1}(w) - \pi_v^{-1}(v)$ pertence a $\mathcal{C}$, pois é apenas a primeira coordenada do produto $(-\pi_v^{-1}(v), \pi_v)(w, \pi_w)$, que pertence a $\Omega(\pi)$.

Em outras palavras, códigos propelineares estão em bijeção com subgrupos Ω de $\mathbb{S}(\mathbb{Z}_2^n)$ que podem ser descritos como grafos $\Omega = \{(v, \pi_v) | v \in \mathcal{C}\}$ para algum código $\mathcal{C}$ de $\mathbb{Z}_2^n$. Isto termina a demonstração. ■

Este lema leva à caracterização dos códigos propelineares via grupos de simetrias.

Teorema 11 *Um código binário $\mathcal{C}$ que contém o vetor nulo possui uma estrutura propelinear se e só se existe um subgrupo N de $\mathbb{S}(\mathbb{Z}_2^n)$ tal que $\mathcal{C} = N(0)$ and $|\mathcal{C}| = |N|$ (ou seja, N age livremente em $\mathcal{C}$).*

Demonstração. Suponha que $\mathcal{C} \subseteq \mathbb{Z}_2^n$ é propelinear; então o grafo $\Omega(\pi)$ é um subgrupo de $\mathbb{S}(\mathbb{Z}_2^n) \cong \mathbb{Z}_2^n \rtimes S_n$. A aplicação $f \mapsto f(0)$ define um rotulamento de $\mathcal{C}$ por $\Omega(\pi)$ e induz uma ação livre e transitiva de $\Omega(\pi)$ em $\mathcal{C}$, dada por $(v, \pi_v)(u) = v + \pi_v(u)$. De fato, é claro que a ação é transitiva e, como $|\mathcal{C}| = |\Omega(\pi)|$, a ação é livre.

Reciprocamente, suponha que N é subgrupo de $\mathbb{S}(\mathbb{Z}_2^n)$, com $\mathcal{C} = N(0)$, $|\mathcal{C}| = |N|$. Das hipóteses sobre N e $\mathcal{C}$ segue que, para cada $v \in \mathcal{C}$, existe um único $f \in N$ tal que $f(0) = v$. Seja $\bar{\pi} : \mathbb{Z}_2^n \rtimes S_n \to S_n$ o homomorfismo $(v, \pi) \to \pi$. Então a aplicação $\pi : C \to S_n$ é dada por $\pi(v) = \pi(f(0)) := \bar{\pi}(f)$. ■

Deste modo, podemos construir exemplos destes códigos via rotulamentos. Para isto, vamos identificar $\mathbb{Z}_2^n$ com os vértices do cubo euclidiano $[-1, 1]^n$ pela aplicação

$$\begin{array}{rccc} \eta: & \mathbb{Z}_2^n & \longrightarrow & \mathbb{R}^n \\ & (a_1, \ldots, a_n) & \mapsto & ((-1)^{a_1}, \ldots, (-1)^{a_n}) \end{array}$$

Esta função não é uma isometria, mas estabelece um isomorfismo entre simetrias do cubo e de $(\mathbb{Z}_2^n, d)$: se f é simetria do cubo, $\eta^{-1} f \eta$ é simetria do espaço de Hamming (detalhes na seção 4.3.4).

Exemplo 7 *Todo código linear C é propelinear, com estrutura dada por $N = C$. Também todo quaternário é propelinear, com estrutura dada por $N = \left(\Phi^{-1}(C), +\right) \subset (\mathbb{Z}_4, +)$*[1].

Exemplo 8 *Considere a álgebra de Clifford real Cl_n. Esta álgebra é construída da seguinte forma: seja $\beta = \{e_1, e_2, \ldots, e_n\}$ uma base ortonormal de $\mathbb{R}^n$. A álgebra de Clifford Cl_n é a álgebra real gerada por $\mathbb{R}^n$ onde o produto é definido pelas equações $e_i e_j = -e_j e_i$, $e_i^2 = -\mathbf{1}$. Pode-se verificar que $\beta(n) = \{\mathbf{1}\} \cup \{e_{i_1} e_{i_2} \ldots e_{i_k}, i_1 < i_2 < \ldots < i_k, 1 \leq k \leq n\}$ é uma base de Cl_n, que portanto possui dimensão 2^n. Podemos identificar Cl_n com $\mathbb{R}^{2^n}$ de modo a levar $\beta(n)$ em uma base ortonormal. Procedendo deste modo, obtemos um grupo de transformações ortogonais dado por $G(n) = \beta(n) \cup -\beta(n)$, que é um subgrupo multiplicativo de Cl_n de 2^{n+1} elementos. O importante é que este grupo mantém invariante o conjunto de vértices $C(n)$ do cubo unitário $C_n = \left\{\sum_{v \in \beta(n)} a_v v | -1 \leq a_v \leq 1\right\}$, pois está contido no grupo $\mathbb{Z}_2^{2^n} \rtimes S_{2^n}$ e age livremente naquele conjunto. Logo, o código $\mathcal{C}_n = \eta^{-1}\left(\left\{g\left(\sum_{v \in \beta(n)} v\right); g \in \beta(n)\right\}\right)$ é propelinear, com estrutura propelinear dada por $N = G(n)$.*

Quando $n = 1$, $G(1)$ é isomorfo a $\mathbb{Z}_4$,e isto corresponde ao rotulamento de Gray utilizado em códigos quaternários. Quando $n = 2$, o grupo $G(2)$ é isomorfo ao grupo dos quatérnios $\mathbb{Q}_8$, e $\mathcal{C}_n = \{(a_1, a_2, a_3, a_4) \mid \sum a_i = 0\}$, que é o código linear $[4, 3, 2]$. Este último exemplo é apresentado em [38], e sua importância vem da classificação dos códigos propelineares invariantes por translação, o tema do artigo mencionado. O que se mostra é que um código propelinear invariante por translação possui uma estrutura propelinear que é um subgrupo do produto direto de grupos $\mathbb{Z}_2^{n_1}$, $\mathbb{Z}_4^{n_2}$ e $\mathbb{Q}_8^{n_3}$.

3.3 Códigos G-lineares e códigos propelineares

Os códigos G-lineares são uma extensão da $\mathbb{Z}_4$-linearidade centrada em grupos de simetrias. Como explicado anteriormente, esta extensão é feita considerando-se um código quaternário mais como um rotulamento do que como a imagem de um código por isometria entre módulos. Este conceito foi introduzido em [19] para códigos em espaços métricos em geral. Códigos G-lineares em espaços de Lee foram estudados em [19, 13, 30, 28], e no Capítulo 2 deste trabalho construímos um rotulamento que pode ser usado para a construção de códigos deste tipo em espaços de Lee.

Os códigos G-lineares podem ser definidos para uma larga classe de espaços métricos que inclui os espaços de Lee e de Hamming. Aqui nós nos restringiremos aos códigos G-lineares em espaços de Hamming binários, mas a mesma definição pode ser feita para outros espaços usuais.

Definição 21 *Seja G um subgrupo de $\mathbb{S}(\mathbb{Z}_2^n, d)$ que age livre e transitivamente em $\mathbb{Z}_2^n$. Considere a extensão canônica da ação de G a uma ação de G^k em $(\mathbb{Z}_2^{kn}, d)$, e considere a aplicação avaliação dada por $s_0(g) = g(0)$. Um código C contido em $\mathbb{Z}_2^{kn}$ é dito* G-linear *se este código for imagem por s_0 de um subgrupo H de G^k.*

[1] Φ é a aplicação de Gray $\Phi : \mathbb{Z}_4^n \to \mathbb{Z}_2^{2n}$.

Deste modo, na G-linearidade o passo inicial é estudar os rotulamentos do espaço ambiente. Nisto se diferencia da propelinearidade, pois nesta última se procuram rotulamentos de um código, e não do espaço inteiro. Um exemplo não-trivial de rotulamento do espaço de Hamming é o que segue:

Exemplo 9 *Para $n = 3$, $\mathbb{S}(\mathbb{Z}_2^3, d)$ é o grupo de simetrias de um cubo, que possui 48 elementos. Os subgrupos G de $\mathbb{S}(\mathbb{Z}_2^3, d)$ que são isomorfos a $\mathbb{Z}_4 \times \mathbb{Z}_2$ ou ao grupo diedral $\mathbb{D}_4$ são os únicos subgrupos rotuladores do cubo (além do grupo $G = \mathbb{Z}_2^3$ que age por reflexões no cubo, que correspondem às translações de $\mathbb{Z}_2^3$).*

Uma ação Ψ de $\mathbb{Z}_4 \times \mathbb{Z}_2$ em $\mathbb{Z}_2^3$ pode ser definida pelo isomorfismo seguinte: dado (a, b) em $\mathbb{Z}_4 \times \mathbb{Z}_2$, $g(a, b)$ é a transformação ortogonal

$$g(a,b) = \begin{bmatrix} \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}^a & 0 \\ 0 & (-1)^b \end{bmatrix}, \quad \Psi(a,b) \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix} := g(a,b) \begin{pmatrix} v_1 \\ v_2 \\ v_3 \end{pmatrix}.$$

O grupo de matrizes obtido é gerado por uma rotação de quarto de volta $R_{\frac{\pi}{2}} = g(1,0)$ em torno do eixo vertical passando pelo centro do cubo e pela reflexão $g(0,1)$ no plano horizontal (passando pelo centro). Nas coordenadas canônicas de $\mathbb{Z}_2^3$ a ação Ψ pode ser escrita do seguinte modo: para $(a,b) \in \mathbb{Z}_4 \times \mathbb{Z}_2$ e $(v_1, v_2, v_3) \in \mathbb{Z}_2^3$, $\Psi(a,b)(v_1, v_2, v_3) = (\widetilde{\phi}(a)(v_1, v_2), b + v_3)$, onde $\widetilde{\phi}$ é a ação associada à aplicação de Gray ϕ. Ou seja, Ψ é a soma da ação de $\mathbb{Z}_4$ dada por $\widetilde{\phi}$ e a ação de $\mathbb{Z}_2$ gerada por τ_{e_3}.

Podemos também definir uma ação de $\mathbb{D}_4$ em $\mathbb{Z}_2^3$. Considere novamente a rotação $R_{\frac{\pi}{2}}$, e também a rotação ρ de ângulo π em torno do eixo horizontal $\overrightarrow{Oy}$ - em coordenadas, $\rho(v_1, v_2, v_3) = (-v_1, v_2, -v_3)$. O grupo gerado por $R_{\frac{\pi}{2}}$ e ρ é isomorfo ao grupo diedral $\mathbb{D}_4$, que possui a apresentação $\mathbb{D}_4 = \langle r, s | r^4 = s^2 = id, srs = r^{-1} \rangle$, sendo um isomorfismo a extensão da aplicação que leva r em $R_{\frac{\pi}{2}}$ e s em ρ. Esta ação é livre e $\mathbb{D}_4$ tem oito elementos; portanto, $\mathbb{D}_4$ rotula $\mathbb{Z}_2^3$, e podemos falar em códigos $\mathbb{D}_4$-lineares.

Exemplo 10 *Para $n \geq 4$, podemos sempre somar as ações definidas acima, obtendo, por exemplo, os códigos $\mathbb{Z}_2^{n_1} \times \mathbb{Z}_4^{n_2}$-lineares.*

Além destes, temos um rotulamento de $\mathbb{Z}_4^2$ pelo grupo $\mathbb{Q}_8 \rtimes \mathbb{Z}_2$. Para isto usaremos a ação de $\mathbb{Q}_8$ definida no Exemplo 8. Para manter a notação usual, faremos $e_1 = \mathbf{i}$, $e_2 = \mathbf{j}$, $e_1 e_2 = \mathbf{k}$. Vimos anteriormente que o conjunto $C = \{\pm\mathbf{1} \pm \mathbf{i} \pm \mathbf{j} \pm \mathbf{k}\}$ é invariante sob $\mathbb{Q}_8$, e que este grupo rotula o subconjunto $C' = \{a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} | a + b + c + d = 0 \bmod 2\}$. Mas também temos que C é invariante sob a conjugação quaterniônica J, onde $J(a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k}) = a\mathbf{1} - b\mathbf{i} - c\mathbf{j} - d\mathbf{k}$; desta maneira, podemos tomar o grupo $\mathbb{G}$ gerado por $\mathbb{Q}_8$ e J, que ainda preserva C. O grupo $\mathbb{G}$ tem $\mathbb{Q}_8$ como subgrupo normal, e $\mathbb{G}$ é isomorfo ao produto semi-direto $\mathbb{Q}_8 \rtimes \mathbb{Z}_2$, onde $\mathbb{Z}_2$ age como a conjugação em $\mathbb{Q}_8$. O grupo $\mathbb{G}$ rotula o conjunto C, e assim pode-se construir códigos $\mathbb{Q}_8 \rtimes \mathbb{Z}_2$-lineares. Note que os códigos propelineares com grupo estrutural $\mathbb{Q}_8$ também são $\mathbb{Q}_8 \rtimes \mathbb{Z}_2$-lineares.

Do Teorema 11 vem a conexão entre G-linearidade e propelinearidade. De fato, um código G-linear $\mathcal{C}$ é rotulado por um subgrupo H de G^k, onde G^k age livre e transitivamente em $(\mathbb{Z}_2^{kn}, d)$. Logo, $\mathcal{C}$ satisfaz as condições do teorema com $N = H$.

Teorema 12 *Todo código G-linear binário é também propelinear.*

A recíproca é falsa: a propelinearidade leva em conta grupos que não podem ser considerados em códigos G-lineares. Note que $|G| = 2^n$, e daí qualquer código G-linear binário tem de ter 2^k palavras, para algum k.

3.4 Códigos Propelineares Invariantes por Translação

Os códigos propelineares invariantes por translação foram definidos e classificados em [38]. Estes códigos, que incluem os códigos lineares e quaternários, são caracterizados pela seguinte propriedade: todas as isometrias de seus grupos rotuladores possuem função deslocamento constante - ou seja, comportam-se como translações. Relembrando, a função deslocamento d_g de uma isometria g é a função $d_g(x) = d(gx, x)$. Se g é uma translação τ_u, é claro que d_g é constante e igual a $d(u, 0)$. Em espaços de Hamming binários, a recíproca é falsa: existem outras isometrias que possuem função deslocamento constante.

Em [38], os códigos propelineares invariantes por translação são classificados; mostra-se que eles são do tipo $\mathbb{Z}_2^{n_1} \times \mathbb{Z}_4^{n_2} \times \mathbb{Q}_8^{n_3}$. Isto é, se o código $\mathcal{C}$ admite uma estrutura propelinear com um grupo N que só possui pseudo-translações, então existe uma estrutura propelinear para $\mathcal{C}$ que é dada por um subgrupo N' de $\mathbb{Z}_2^{n_1} \times \mathbb{Z}_4^{n_2} \times \mathbb{Q}_8^{n_3}$.

No exemplo 10, vimos que códigos rotulados por $\mathbb{Q}_8$ são $\mathbb{Q}_8 \rtimes \mathbb{Z}_2$-lineares. Claramente, um código de tipo $\mathbb{Z}_2^{n_1} \times \mathbb{Z}_4^{n_2} \times \mathbb{Q}_8^{n_3}$ também é $\mathbb{Z}_2^{n_1} \times \mathbb{Z}_4^{n_2} \times (\mathbb{Q}_8 \rtimes \mathbb{Z}_2)^{n_3}$-linear ou, de modo equivalente, é soma direta de um código linear, outro $\mathbb{Z}_4$-linear e um terceiro $(\mathbb{Q}_8 \rtimes \mathbb{Z}_2)$-linear. Deste modo, todo código propelinear invariante por translação é também G-linear.

Finalmente, observamos que não vale a recíproca. Por exemplo, o grupo diedral $\mathbb{D}_4$ é um grupo parametrizador de $\mathbb{Z}_2^3$, como descrito no exemplo 9.

Resumindo, as relações entre propelineares e G-lineares são as seguintes:

Teorema 13 *Para códigos binários, valem as inclusões estritas:*
Propelinear invariante por translação $\subset$ *G-linear* $\subset$ *Propelinear.*

3.4.1 Propelineares em outros alfabetos

Podemos considerar estes tipos de códigos em qualquer espaço (A^n, d), com A um grupo abeliano, d a distância de Hamming. Uma extensão natural da propelinearidade considerada em [2] é a seguinte:

Definição 22 *Um código C em A^n contendo* 0 *é* propelinear *se existe um subgrupo N de $A^n \rtimes S_n$ que age de modo regular em C.*

Observe que o grupo $A^n \rtimes S_n$ é um subgrupo do grupo de simetrias de (A^n, d). Como antes, definimos

Definição 23 *(C, N) é invariante por translação se todo elemento g de N tem função deslocamento d_g constante.*

Um problema interessante é descrever a classe dos códigos invariantes por translação em alfabetos não-binários. Na verdade esta classificação é muito simples: são todos *lineares*, e não existe outra estrutura propelinear possível. Este é um resultado que estende um teorema provado em [3] para $A = \mathbb{Z}_m$.

Teorema 14 *Sejam A um grupo abeliano, $|A| > 2$, (A^n, d) espaço de Hamming sobre A^n, $n > 1$. Então um código C é propelinear invariante por translação se e só se é linear, e a única estrutura propelinear (C, N) para C é dada por sua estrutura linear (N é C considerado como grupo de translações).*

Demonstração. Mostraremos que, se $g = \tau_v \pi \in A^n \rtimes S_n$, então d^g é constante se, e somente se, $\pi = id$.

Suponha que $\pi \neq id$. Os suportes de τ_v e π são os conjuntos

$$supp(\pi) = \{i \in \{1, 2, ..., n\} | \pi(i) \neq i\},$$
$$supp(\tau_v) = \{i \in \{1, 2, ..., n\} | v_i \neq 0\}, \quad \text{onde } v = (v_1, \ldots, v_n).$$

Três casos são possíveis.

(i) Os suportes são disjuntos. Neste caso, sejam $i \in supp(\pi)$ e $v_i e_i = (0, ..., 0, v_i, 0, ..., 0)$. Temos que $w(v + \pi(v_i e_i) - v_i e_i) = w(v) + 2$, e d^g não é constante.

(ii) Existe um índice i tal que $i \in supp(\pi) \cap supp(\tau_v)$.

(ii.i) Suponha que $\pi_v(i) \in supp(\tau_v)$.Então temos

$v + \pi(v_i e_i) - v_i e_i = (v_1, ...v_{i-1}, 0, v_{i-2}, ..., v_{\pi(i)} + v_i, ..., v_n)$, e claramente

$$w(v + \pi_v(v_i) - v_i) \leq w(v) - 1.$$

(ii.ii) Finalmente, suponha que $i \in supp(\pi) \cap supp(\tau_v)$ e que $\pi_v(i) \notin supp(v)$. Escolha $v_i' \in A$ tal que $v_i' \neq v_i, v_i' \neq 0$ (note que isto não é possível no caso binário). Então,

$$w(v + \pi_v(v_i' e_i) - v_i' e_i) = w(v) + 1.$$

Isto mostra que, se d^g é constante, então $supp(\pi)$ deve ser vazio. Ou seja, g é uma translação pura. ■

Capítulo 4

Rotulamentos Cíclicos em Espaços de Hamming

4.1 Introdução

Os bons resultados obtidos com os códigos quaternários foram um primeiro impulso para o estudo de códigos sobre anéis. Esta generalização – códigos em módulos com pesos – pode ser proveitosa para o estudo de códigos em espaços de Hamming, bastando que exista uma isometria do módulo em um espaço(F_q, d).

Naturamente, para cada novo espaço métrico temos um novo problema de teoria de códigos, e por isso os anéis $\mathbb{Z}_{p^k}$ e a técnica do levantamento de Hensel adquiriram importância: por este método pode-se construir uma sequência de códigos C_k em $\mathbb{Z}_{p^k}^n$ a partir de um código em $\mathbb{Z}_p^n$. Também por isso os anéis $\mathbb{Z}_{p^k}$ têm estado no centro de trabalhos recentes sobre códigos em módulos.[1]

Para imitar fielmente a construção dos quaternários, desejaríamos obter rotulamentos cíclicos de espaços de Hamming. Infelizmente a situação é a mesma que a dos espaços de Lee: não há nenhum rotulamento além do de $\mathbb{Z}_2^2$ por $\mathbb{Z}_4$. Isto já havia sido provado em [39] para $\left(\mathbb{Z}_p^k, d\right)$, e a extensão para alfabetos quaisquer é feita aqui na próxima seção.

Por outro lado, existem vários trabalhos sobre pesos em anéis e a realização destes como códigos em espaços de Hamming. Existem basicamente duas isometrias: uma de $\left(\mathbb{Z}_{p^2}, w_{\text{hom}}\right)$ em um código MDS $[p, 2]$ fixado, e outra, a mais utilizada, de $(\mathbb{Z}_{p^n}, w_{\text{hom}})$ no código de Reed-Muller de primeira ordem. O peso w_{hom} mencionado é chamado de peso homogêneo em [16]

[1] O levantamento de Hensel funciona para códigos cíclicos apenas. O termo "cíclico" não se refere a rotulamentos cíclicos, mas sim a códigos invariantes sob a permutação $(a_1, a_2, \ldots, a_n) \mapsto (a_n, a_1, \ldots, a_{n-1})$. Estes códigos podem ser vistos comos *ideais* no anel $R_n = F[x]/(x^n - 1)$: identificando $(a_1, a_2, \ldots, a_n)$ com $a_1 + a_2 x + \ldots + a_n x^{n-1}$, vê-se que a permutação acima coincide com a multiplicação por x em R_n. Os ideais de R_n são quocientes $I/(x^n - 1)$, onde I é um ideal de $F[x]$ que contém o ideal gerado por $x^n - 1$. Como cada ideal de $F[x]$ é gerado por um polinômio $f(x)$, os ideais de R_n são gerados por polinômios que dividem $x^n - 1$ Para $F = \mathbb{Z}_p$, o levantamento de Hensel do código $C = (f) \subset R_n$ é o código definido em $\mathbb{Z}_{p^k}[x]/(x^n - 1)$ pelo único polinômio mônico $\overline{f}$ que divide $(x^n - 1)$ e que é pré-imagem de f (veja, p.ex., [8]).

e [21], sendo definido de modo que os elementos do ideal $p^{n-1}\mathbb{Z}_{p^n}$ tenham peso máximo nos códigos mencionados. Como resultados nesta área, citamos os levantamentos do código ternário de Golay para $\mathbb{Z}_9$ [21], do código binário de Golay para $\mathbb{Z}_8$ [17], e a generalização dos códigos de Delsarte-Goethals para $\mathbb{Z}_{2^k}$ [9]. Em todos estes casos são obtidos códigos não-lineares com parâmetros melhores do que os anteriormente existentes.

Neste capítulo nós iremos analizar as isometrias citadas do ponto de vista de rotulamentos. Além de fornecer um modo mais construtivo de realizar estas isometrias, nosso estudo chama a atenção para um fato que passou despercebido: os códigos utilizados possuem simetrias que não podem ser estendidas ao espaço ambiente. Longe de ser apenas uma curiosidade, a existência de tais isometrias torna bem mais complicado o cálculo da dimensão necessária para a realização de um espaço $(\mathbb{Z}_{p^k}, w)$ como código e, em particular, entra de modo vital na isometria entre $(\mathbb{Z}_{2^k}, w_{\text{hom}})$ e o código de Reed-Muller. De fato, as isometrias deste código que provêm do espaço de Hamming não podem parametrizá-lo, pois se a ordem da isometria é 2^m, então m não pode ser superior a $k-1$. Outros códigos já foram estudados em relação à questão da existência de isometrias não-extensíveis [40]. Códigos cujas isometrias são todas provenientes de $\mathbb{S}\left(F_q^n, d\right)$ são chamados metricamente rígidos - ou seja, $\mathbb{S}(C) = \mathbb{S}\left(C, F_q^n\right)$, na notação da seção 1.2. Como subproduto dos cálculos feitos, concluímos que os códigos binários de Reed-Muller não são metricamente rígidos.

As construções e cálculos começam por considerar as "coordenadas corretas" nos códigos de Reed-Muller: cada ponto corresponde a um par (f, c), onde f é um funcional linear e c é uma constante. Disto nós partimos para associar grafos a estes códigos e calcular os grupo de simetrias. O caso binário é especial, e neste utilizamos a correpondência entre o código de Reed-Muller em $\mathbb{Z}_2^{2^m}$ e o código biortogonal em $\mathbb{R}^{2^m}$. Boa parte dos resultados apresentados aqui pode ser encontrada no artigo "Labelings of Lee and Hamming spaces" [28], escrito em conjunto com Suei Costa. A demonstração da inexistência de rotulamentos cíclicos do espaço de Hamming encontra-se no relatório de pesquisa [29], também feito com Sueli Costa. A estes acrescentamos a descrição dos grupos de simetrias dos códigos de Reed-Muller de primeira ordem e dos códigos MDS $[p, 2]$, e fornecemos estimativas para ordens de simetrias em $\left(\mathbb{Z}_p^{p^n}, d_h\right)$.

4.2 Rotulamentos cíclicos de espaços de Hamming

Nesta seção mostraremos que rotulamentos cíclicos em espaços de Hamming só existem para comprimento 1 ou para $\left(\mathbb{Z}_2^2, d_h\right)$, onde temos o rotulamento de Gray. Isto não depende em nada da estrutura algébrica do alfabeto. Por isso, vamos tomar como alfabeto simplesmente um conjunto não-vazio X.

Este resultado complementa um teorema análogo para espaços de Lee: estes não admitem parametrizações cíclicas, a menos dos casos triviais já mencionados costalee. Na verdade, nem parametrizações abelianas distintas do grupo de translações são possíveis [30, 28]. No caso de Hamming, existem parametrizações abelianas distintas do grupo de translações, mas ainda não é claro como estas podem ser usadas em códigos. Em particular, nos espaços binários tais

parametrizações não podem ser feitas, e não se sabe se existem outras (além das fornecidas pela aplicação de Gray da $\mathbb{Z}_4$-linearidade).

Enfim, este resultado mostra que com grupos cíclicos só se pode parametrizar códigos próprios, e não o espaço todo. Estimativas em casos especiais – comprimento igual a p^n, p primo – serão fornecidas mais adiante (Seção 4.3.2), onde veremos que também há sérias limitações quanto à taxa de tais códigos.

A demonstração é longa, mas usa apenas um resultado básico sobre a estrutura de um grupo cíclico e algumas características geométricas do espaço de Hamming. No espaço de Hamming (X^n, d) nós consideraremos as "retas" $X_{i,p}$ passando por um ponto p que são dadas por

$$X_{i,p} = \{(p_1, \ldots, p_{i-1}, x, p_{i+1}, \ldots, p_n) | x \in X\}.$$

Lema 5 *Seja p um ponto de X e seja $B_1(p)$ a bola unitária centrada em p. Para qualquer ponto q de X, temos*

(H1) *$d(p,q) = 1$ se e só se $B_1(p) \cap B_1(q) = X_{i,p} = X_{i,q}$ para algum índice i;*

(H2) *$d(p,q) = 2$ se e só se $B_1(p) \cap B_1(q)$ é um conjunto de dois pontos distintos.*

Isto é consequência direta da definição de métrica de Hamming. Estas equivalências serão muito usadas no que segue. Além destas, precisaremos também do seguinte resultado sobre grupos cíclicos:

Teorema 15 *Seja G um grupo cíclico, e seja g um elemento de G diferente da identidade. Então o subgrupo gerado por g consiste dos elementos de G cujas ordens dividem a ordem de g.*

Daqui em diante fixaremos o ponto $p = (p_1, p_2, \ldots, p_n)$, e por isso usaremos a notação X_i no lugar de $X_{i,p}$.

Lema 6 *Seja g uma isometria de (X^n, d) , $m > 2$, e seja G o subgrupo gerado por g, $G = \langle g \rangle$. Então*

(i) *Se os pontos $p, g^t(p)$ e $g^s(p)$ são distintos, e tanto $g^t(p)$ como $g^s(p)$ estão na mesma reta X_i, então $g^{t-s}(p)$ também está em X_i.*

(ii) *Seja G um subgrupo de isometrias que age livremente em X^n. Se $g(p)$ e $g^2(p)$ se encontram na mesma reta X_i, então a órbita de p sob G, $G(p) = \{g^k(p) | k = 1, 2, \ldots, |g|\}$, está contida em X_i. Caso $g(p)$ esteja em X_i mas $g^2(p)$ não, os únicos pontos de intersecção desta órbita com X_i são p e $g(p)$.*

Demonstração.

(i) Por hipótese, $d(g^t(p), g^s(p)) = 1$ e $d(g^s(p), p) = 1$. Portanto,

$$d(g^{t-s}(p), p) = d(g^t(p), g^s(p)) = 1$$

e também

$$d(g^{t-s}(p), g^t(p)) = d(g^{-s}(p), p) = d(p, g^s(p)) = 1.$$

Isto mostra que $g^{t-s}(p) \in B_1(p) \cap B_1\left(g^t(p)\right)$. Pelo Lema 5, $B_1(p) \cap B_1\left(g^t(p)\right) = X_i$, e $g^{t-s}(p) \in X_i$.

(ii.a) Suponha que os pontos $g(p)$ e $g^2(p)$ pertencem à reta X_i. Como G age livremente, $g^k(p) \neq g^l(p)$ se $k \neq l$ e $0 < k, l \leq |g|$. Para $k = |g| - 1$, temos

$$g^{|g|-1}(p) = g^{-1}(p) = g^{1-2}(p) \in X_i$$

por (i). Para todos os outros k entre 1 e $|g| - 2$ podemos aplicar indução em k: se $g^k(p) \in X_i$, então $g^{k+1}(p) = g^{k-(-1)}(p) \in X_i$. Isto mostra que a órbita $G(p)$ está contida em X_i.

(ii.b) Agora, se $g(p) \in X_i$ mas $g^2(p) \notin X_i$, seja $t > 2$ o primeiro inteiro positivo tal que $g^t(p)$ pertence a X_i; mostraremos que $t = |g|$, e portanto, que $g^t(p) = p$. Observe que a ordem de g é maior do que 2, pois senão $g^2(p) = p$ pertenceria a X_i.

Certamente $g^t(p) \neq g(p)$, pois senão teríamos $g^{t-1}(p) = p$, em contradição com a escolha de t. Por outro lado, se $g^t(p) \neq p$, os pontos $p, g(p), g^t(p)$ são todos distintos e estão em X_i. Por (i), o ponto $g^{t-1}(p)$ também pertence a X_i, contradição novamente. Então $g^t(p) = p$, o que implica em $g^t = id$, e a intersecção de $G(p)$ com X_i consiste dos pontos p e $g(p)$. ■

Teorema 16 *Seja (X^n, d) o espaço de Hamming sobre X^n, onde $|X| = m$. Se $(m, n) \neq (2, 2)$ e $n > 1$, não existe nenhum rotulamento cíclico de (X^n, d).*

Demonstração. A demonstração se quebra naturalmente em dois casos, $m = 2$ e $m > 2$. Observamos que o caso binário já é tratado em [39] por métodos diferentes.

1. Começaremos pelo caso $m > 2$. Suponha que existe um grupo cíclico G que rotula X^n, e seja g um gerador deste grupo. Vamos mostrar que $n = 1$.

Para cada reta X_i, seja k_i o menor inteiro positivo tal que $g^{k_i}(p)$ pertence a esta reta. Seja G_i o subgrupo de G gerado por g^{k_i}, $G_i = \left\{g^{sk_i}; 0 \leq s < m^n/k\right\}$.

1.1 Suponha que $g^{2k_1}(p)$ não pertence a X_1.

Pelo lema 6.ii, $G_1(p) \cap X_1 = \{p, g^{k_1}(p)\}$. Como $m > 2$, existe um ponto q em X_1 que é distinto de p e de $g^{k_1}(p)$. Como G rotula X^n, existe um expoente $t, 0 < t < m^n$, tal que $g^t(p) = q$. O lema 6.i assegura que $g^{t-k_1}(p)$ também é um ponto de X_1. Por outro lado, temos

$$d(g^{t-k_1}(p), g^{-k_1}(p)) = d(g^t(p), p) = 1.$$

Como $d(g^{-k_1}(p), p) = d(g^{k_1}(p), p) = 1$, mas $g^{-k_1}(p)$ não pertence a X_1, necessariamente $g^{-k_1}(p) = (p_1, \ldots, p_{j-1}, a, p_{j+1}, \ldots, p_n)$ com $a \neq p_j$ e $j \neq 1$. Logo, $g^{t-k_1}(p)$ pertence à intersecção da bola $B_1(g^{-k_i}(p))$ com a reta X_1; mas $B_1(g^{-k_i}(p)) \cap X_1 = \{p\}$, e segue que $g^{t-k_1}(p) = p$. Ou seja, $q = g^t(p) = g^{k_1}(p)$, absurdo. Portanto $G(p) \cap X_i = G_i(p) \cap X_i = \{p, g^{k_1}(p)\}$ e não temos um rotulamento, contradição novamente. Logo, é necessário que $g^{2k_1}(p)$ pertença a X_1.

1.2 Vamos agora mostrar que a condição $g^{2k_1}(p) \in X_1$ implica em $G_1(p) = X_1$.

Pelo Lema 6.ii já sabemos que $G_1(p) \subset X_1$. Para mostrar a recíproca, seja v um ponto de X_1 e seja l tal que $0 \leq l < m^n$ e $g^l(p) = v$. Existe um inteiro não negativo s tal que $sk_1 \leq l < (s+1)k_1$ ou, em outras palavras, $0 \leq l - sk_1 < k_1$. Suponha que $l \neq sk_1$. Então o Lema 6.i garante que $g^{l-sk_1}(p) \in X_1$, mas a minimalidade de k_1 implica em $l - sk_1 = 0$,

contradição. Portanto $g^l = g^{sk_1}$ e g^l pertence a G_1. Isto mostra que $G_1(p) = X_1$. Isto também implica em $|G_1| = m$, porque a ação de G é livre, e daí e do Teorema 15 segue que $G_1 = \left\langle g^{m^{n-1}} \right\rangle$.

Neste caso, pode n ser maior que 1? Certamente que não. Suponha que $n > 1$ e seja $1 < j \leq n$. Não podemos ter $g^{2k_j}(p)$ em X_j porque as mesmas contas nos levariam a $|G_j| = m$ e, usando o Teorema 15, obteríamos $G_j = \left\langle g^{m^{n-1}} \right\rangle = G_1$. Também não pode ocorrer que $g^{2k_j}(p)$ não pertença a X_j (como vimos acima), pois isto leva a $X_j = G(p) \cap X_j = \{p, g^{k_j}(p)\}$, absurdo ($|X_j| > 2$). Conclusão: $n = 1$, e $G_1 = \langle g \rangle = G \cong \mathbb{Z}_m$.

2. No caso binário nós identificaremos X^n com $\mathbb{Z}_2^n$ e p com a origem. Isto é apenas para facilitar a notação, pois a única estrutura algébrica utilizada na demonstração é a de G.

Sejam g e G como antes, $\beta = \{e_1, \ldots, e_n\}$ a base canônica de $\mathbb{Z}_2^n$, e seja k tal que $g^k(0) = e_1$, $0 < k < 2^n$. Veremos que as únicas possibilidades são $n = k = 1$ ou $n = 2$ e $k = 1$ ou 3 (que é um rotulamento por $\mathbb{Z}_4$).

2.1 Suponha que $|g^k| > 2$; então $g^{-k} \neq g^k$, o que implica em $g^{-k}(0) = e_j$ para algum $j \neq 1$. Seja l tal que $g^l(0) = e_1 + e_j$. Nós temos $d(g^{l+k}(0), g^l(0)) = d(g^k(0), 0) = 1$ e também $d(g^{l+k}(0), 0) = d(g^l(0), g^k(0)) = 1$. Disso podemos concluir

$$g^{l+k}(0) \in S_1(0) \cap S_1(g^l(0)) = \{g^k(0), g^{-k}(0)\} \Longrightarrow g^{l+k} = g^{\pm k}.$$

Sendo assim, ou $g^l = g^0 = id$ – o que implica em $0 = e_1 + e_j$, absurdo, ou $g^l = g^{2k}$, que é a resposta correta. O mesmo raciocínio aplicado a g^{l-k} em lugar de g^{l+k} fornece a equação $g^l = g^{-2k}$, i.e., $g^{2k} = (g^{2k})^{-1}$, e portanto g^{2k} é um elemento de ordem 2. Logo, g^k tem ordem 4.

Pelo Teorema 15 sabemos que todo elemento de ordem quatro pertence ao grupo $\left\langle g^{2^{n-2}} \right\rangle$, que possui apenas dois elementos desta mesma ordem, $g^{2^{n-2}}$ and $g^{3 \cdot 2^{n-2}}$. Então apenas dois pontos da esfera $S_1(0)$ podem ser rotulados por elementos de ordem maior que 2, e_1 e e_j. Se $n > 2$, os outros pontos da esfera unitária precisam ser rotulados por elementos de ordem dois, mas o único elemento de ordem dois é $g^{2^{n-1}}$, que é o elemento g^l. Como a ação de G é transitiva e apenas dois pontos de $S_1(0)$ estão em sua órbita, conclui-se que $n = 2$, $k = 1$ ou 3, e os rotulamentos correspondentes são gerados por uma rotação no sentido horário ou anti-horário, ambos correspondendo a rotulamentos por $\mathbb{Z}_4$.

2.2 Para finalizar a demonstração precisamos examinar o caso $|g^k| = 2$, i.e., $k = 2^{n-1}$. Afirmamos que isto implica em $n = 1$. De fato, vimos acima que qualquer g^t que satisfaça $d(g^t(0), 0) = 1$ tem de possuir ordem 2 ou 4. Caso $|g^t| = 4$, acabamos de ver que $g^{2^{n-1}}(0)$ não pertence a $B_1(0)$. Portanto, se $g^t(0) \in B_1(0)$, então $t = 2^{n-1}$. Como G age transitivamente $n = 1$ e $G = \mathbb{Z}_2$. ■

Em particular, para os espaços de Hamming mais importantes, temos

Corolário 1 *Não existe nenhum rotulamento dos espaços de Hamming $(F_{p^k}^n, d)$ e $(\mathbb{Z}_{p^k}^n, d)$ por $\mathbb{Z}_{p^{kn}}$, exceto para $p = 2, k = 1$ e $n = 2$ (e os rotulamentos triviais quando $n = 1$).*

4.3 Códigos de Reed-Muller de primeira ordem e seus rotulamentos

4.3.1 Os grupos de simetrias

Os códigos de Reed-Muller são códigos lineares definidos sobre o corpo $\mathbb{Z}_2$. Suas extensões para corpos finitos quaisquer são conhecidas por códigos de Reed-Muller generalizados, mas nos referiremos a todos estes simplesmente como códigos de Reed-Muller. Começaremos esta seção pela definição destes códigos (a métrica usada é a de Hamming).

Seja F_q um corpo finito de q elementos, e $F_q[x_1, \ldots, x_m]$ o anel de polinômios sobre F_q a m variáveis. Dentro de $F_q[x_1, \ldots, x_m]$ destacamos certos subespaços vetoriais, que são os espaços

$$R_{r,m} = \{f \in F_q[x_1, \ldots, x_m]; \deg(f) \leq r\}$$

onde $\deg(f)$ é o grau de f. Considere uma ordenação dos vetores de F_q^m, $v_1 < v_2 < \ldots < v_{q^m}$, e seja ϕ a aplicação

$$\begin{array}{rccc} \phi: & F_q[x_1, \ldots, x_m] & \longrightarrow & F_q^{q^m} \\ & f & \longmapsto & (f(v_1), \ldots, f(v_{q^m})) \end{array}$$

O código (generalizado) de Reed-Muller de ordem r sobre F_q, denotado por $GRM(r,m)_q$, é a imagem de $R_{r,m}$ por ϕ. Para o código binário de Reed-Muller usaremos a notação tradicional $RM(r,m)$. Neste trabalho nós nos ocuparemos de $GRM\,(1,m)_q$, o Reed-Muller de primeira ordem. Para não carregar na notação, identificaremos $R_{1,m}$ e $GRM(1,m)_q$: ao invés de escrever $\phi(f)$, escreveremos simplesmente f, a não ser quando for estritamente necessário distinguir o polinômio e sua imagem.

Os polinômios enumeradores dos códigos $GRM(1,m)_q$ são conhecidos e são muito simples de calcular. Os elementos destes códigos são funções afins de m variáveis, ou seja, cada um é a soma de um funcional linear e uma função contante. Enfim, cada funcional tem exatamente q^{m-1} zeros, pois, este é o número de pontos de um hiperplano em F_q^m. Logo, se $f \in GRM\,(1,m)_q$ não é constante, o peso de f é q^{m-1}. Para as constantes, temos a função nula e as outras, de peso q^m. Portanto, o polinômio enumerador é

$$w(x) = 1 + (q^{m+1} - q)x^{q^{m-1}} + (q-1)x^{q^m}.$$

De posse desta informação podemos calcular facilmente o grupo de simetrias de $GRM(1,m)_q$. Para este cálculo usaremos um grafo associado a este código.

Definição 24 *$\Gamma(1,m,q)$ é o grafo que tem por vértices os pontos do código de Reed-Muller de primeira ordem sobre F_q, e cujas arestas são os pares (f,g) tais que $d(f,g) = q^m$.*

Em outras palavras, (f,g) é aresta se e só se $f-g$ é um polinômio constante. Embora o mais natural fosse conectar os pontos mais próximos – isto é, conectar f e g se $d\,(f,g) = q^{m-1}$ – as contas são mais simples com o grafo que definimos. Nesta seção nos referiremos a este grafo por Γ, salvo onde haja possibilidade de confusão.

Proposição 1 *Uma aplicação $\phi : GRM(1,m)_q \to GRM(1,m)_q$ é uma isometria se e só se é um automorfismo de $\Gamma(1,m,q)$.*

Demonstração. Por um lado, é claro que uma isometria é automorfismo. A recíproca também é simples: se f e g são tais que $d(f,g) = q^{m-1}$ e ϕ é um automorfismo, então $d(\phi f, \phi g) = q^{m-1}$, pois só há 3 possibilidades: 0, q^{m-1} ou q^m. Não pode ser 0 ou q^m porque ϕ é automorfismo, e logo só pode ser q^{m-1}. Observe que isto funciona em qualquer código de dois pesos. Segue que o grupo de isometrias de $GRM(1,m)_q$ é igual ao grupo de automorfismos de Γ. ∎

O grafo Γ é uma união disjunta de grafos completos. Para mostrar isso, considere o subespaço $\mathcal{O}_m$[2] de $GRM(1,m)_q$ dado pelos polinômios que têm grau 1 e possuem termo constante nulo, mais o polinômio identicamente nulo. Então o grafo Γ constitui-se de q^{m-1} componentes conexas indexadas por $\mathcal{O}_m$, e cada componente é um grafo completo K_q.

De fato, seja f um elemento de $GRM(1,m)_q$, e seja $K(f)$ a componente que contém f. Como (f,g) é aresta de Γ se e só se $f-g$ é constante, isto é, se e só se $g = f + c$, com $c \in F_q$, temos que $K(f) = \{f + c; c \in F_q\}$. Como $d(f+c_1, f+c_2) = q^m$, $K(f)$ é isomorfo ao grafo completo K_q.Além disso, existe um único c tal que $f + c$ tem termo constante nulo, e por isso podemos indexar as componentes por $\mathcal{O}_m$.

Vamos agora determinar os automorfismos de Γ.

Teorema 17 *O grupo de automorfismos de $\Gamma(1,m,q)$ é isomorfo a $S_q^{q^m} \rtimes S_{q^m}$.*

Demonstração. Considere o grupo de bijeções de $\mathcal{O}_m$, que é isomorfo a S_{q^m}; identificaremos estes grupos no que segue. Podemos estender sua ação para $GRM(1,m)_q$ do seguinte modo: dado $f = f_0 + c$, com $f_0 \in \mathcal{O}_m$ e $c \in F_q$, e π uma permutação de $\mathcal{O}_m$, definimos $\pi(f) = \pi(f_0) + c$. Esta aplicação é um automorfismo de Γ. Basta ver que $d(f,g) = q^m$ se e somente se $f = f_0 + c_1$ e $g = f_0 + c_2$, com $f_0 \in \mathcal{O}_m$ e $c_1 \neq c_2$. Então $d(\pi(f), \pi(g)) = d(\pi(f_0) + c_1, \pi(f_0) + c_2) = d(c_1, c_2) = q^m$.

Fixe agora uma enumeração de $\mathcal{O}_m$, e seja $K(f_i)$ a componente de f_i em Γ. O grupo de automorfismos de $K(f_i)$ é isomorfo a S_q, pois $K(f_i)$ é um grafo completo K_q. Com isto podemos definir uma ação de $S_q^{q^m}$ em Γ da seguinte maneira: dados $\sigma = (\sigma_1, \ldots, \sigma_{q^m}) \in S_q^{q^m}$ e um vetor $f = f_i + c \in GRM(1,m)_q$, então $\sigma(f) = f_i + \sigma_i(c)$. Isto é um automorfismo de Γ: se $f - g$ é constante e diferente de zero, então $f = f_i + c_1$ e $g = f_i + c_2$, e é claro que $\sigma(f) - \sigma(g) = \sigma_i(c_1) - \sigma_i(c_2)$ é constante e não-nula.

Mostremos agora que todo automorfismo de Γ pode ser expresso (de modo único) como um produto de uma permutação de componentes e de um elemento de $S_q^{q^m}$. Primeiro, note que a intersecção destes grupos é o grupo $\{id\}$, o que implica na unicidade da decomposição. Prosseguindo, seja ϕ um automorfismo. Como ϕ é automorfismo, ϕ permuta as componentes $K(f_i)$: $\phi(K(f_i)) = K(f_j)$. Fazendo $j = \pi(i)$, definimos uma permutação de componentes $\pi \in S_{q^m}$. Claramente, temos $\phi\pi^{-1}(K(f_i)) = (K(f_i))$, para todo f_i em $\mathcal{O}_m$.

[2] A notação é motivada pelo caso binário, onde o código $\mathcal{O}_m$ é chamado de código ortogonal. O motivo é que este código corresponde a uma base ortogonal em $\mathbb{R}^{2^m}$.

Agora, como $\phi\pi^{-1}$ fixa as componentes, podemos olhar as restrições correspondentes, isto é, $\phi\pi^{-1}|_{K(f_i)} : K(f_i) \to K(f_i)$. Seja σ_i o elemento de S_q que corresponde a $\phi\pi^{-1}|_{K(f_i)}$, e seja $\sigma = (\sigma_1, \ldots, \sigma_{q^m})$. Então temos $\phi\pi^{-1} = \sigma$, ou seja, $\phi = \sigma\pi$. Mais ainda, temos que $Aut(\Gamma)$ é isomorfo a um produto semi-direto de $S_q^{q^m}$ por S_{q^m}. Para verificar isso, sejam $\pi \in S_{q^m}$, $\sigma \in S_q^{q^m}$, e $f = f_i + c \in GRM(1,m)_q$. Então

$$\begin{aligned} \pi\sigma\pi^{-1}(f_i + c) &= \pi\sigma(f_{\pi^{-1}(i)} + c) \\ &= \pi\left(f_{\pi^{-1}(i)} + \sigma_{\pi^{-1}(i)}c\right) \\ &= f_i + \sigma_{\pi^{-1}(i)}c \\ &= \left(\sigma_{\pi^{-1}(1)}, \ldots, \sigma_{\pi^{-1}(q^m)}\right)(f_i + c), \end{aligned}$$

o que mostra que $S_q^{q^m}$ é normal em $Aut(\Gamma)$ e que a estrutura de $Aut(\Gamma)$ é dada pelo produto semi-direto usual de S_{q^m} por $S_q^{q^m}$: $(\sigma,\pi)(\sigma',\pi') = (\sigma(\sigma')^{\pi}, \pi\pi')$, onde $(\sigma')^{\pi} = \left(\sigma_{\pi^{-1}(1)}, \ldots, \sigma_{\pi^{-1}(q^m)}\right)$. ■

4.3.2 Rotulamentos Cíclicos

Rotulamentos de $GRM(1,m)_q$

A existência de rotulamentos cíclicos para o código de Reed-Muller é uma consequência de um teorema geral sobre isometrias entre anéis e este código. O caso binário havia sido tratado em [9], onde é exibida uma isometria entre $RM(1,m)$ e o anel $(\mathbb{Z}_{2^{m+1}})$ com o peso w dado por $w(0) = 0$, $w(2^m) = 2^m$, e $w(v) = 2^{m-1}$ para $v \neq 0, 2^m$. A isometria mais geral aparece em [21] como uma extensão da anterior para os códigos de Reed-Muller de primeira ordem sobre alfabetos q-ários. O resultado referido é o seguinte:

Teorema 18 *[21] Seja R um anel de cadeia finito (de característica q) e comprimento m. Então existem um peso w em R tal que (R,w) e $GRM(1,m)_q$ são isométricos.*

Como $\mathbb{Z}_{q^{m+1}}$ é um anel de cadeia finito, conclui-se deste teorema e do Lema 1 a existência dos rotulamentos cíclicos de $GRM(1,m)_q$. O peso w em R é uma variação do peso definido no parágrafo anterior. Basicamente, a cadeia de ideais de R é dada por $0 \subset J^m \subset J^{m-1} \subset \ldots \subset J \subset R$, onde J é seu ideal maximal. Os pesos são $w(0) = 0$, $w(r) = q^m$ se $r \in J^m$, e $w(r) = q^{m-1}$ para os demais elementos. Vê-se aí o perfil de pesos de $RM(1,m)_q$, pois $|J^m| = q$.

A descrição das isometrias do código é a base para obter rotulamentos explicitamente dados por simetrias. Considerando uma enumeração de $\mathcal{O}_m$, tomaremos o ponto f_1 como ponto inicial. Sejam π um q^m-ciclo de S_{q^m} e σ' um q-ciclo de S_q. Defina $\sigma = \left(\sigma_1, \ldots, \sigma_{q^m-1}\right) \in S_q^{q^m}$ por

$$\sigma_i = \begin{cases} \sigma', \text{ se } i = 1 \\ id, \text{ caso contrário.} \end{cases}$$

Seja $\phi = \sigma\pi$. Aplicando ϕ seguidamente a f_1 percorremos todo o código de Reed-Muller. De fato, seja $0 < k \leq q^{m+1}$, $k = lq^m + r$, com $0 \leq r < q^m$. Então

$$\phi^k(f_1) = f_{\pi^r(1)} + \left(\sigma'\right)^l(0)$$

Como tanto π quanto σ' são ciclos de ordem máxima, temos $\phi^k(f_1) = f_1$ apenas quando $\kappa = q^{m+1}$. Portanto, isto é de fato um rotulamento cíclico de $GRM(1,m)_q$

Rotulamentos cíclicos do código de Reed-Solomon sobre F_q

Os cálculos feitos podem ser aplicados ao caso do códigos de Reed-Solomon, que também foi estudado como imagem isométrica do anel $\mathbb{Z}_{p^2}$, p primo. Isometrias entre $\mathbb{Z}_{p^2}$ e códigos MDS do tipo $[p,2]$ foram construídas em [16], e esta construção foi estendida para anéis de Galois $GR\left(q^2,p^2\right)$ e códigos MDS $[q,2]$ em F_q^q, como pode ser visto em [23], pp.220-222 (ver também [33])[3]. Nesta parte nós faremos rotulamentos do código MDS de Reed-Solomon pelo grupo $\mathbb{Z}_{q^2}$, $q = p^k$.

Definição 25 *Seja L o espaço dos polinômios de grau 1 em uma variável sobre F_q. Considere a aplicação de avaliação*

$$\begin{array}{rccc} \phi: & F_q[x] & \longrightarrow & F_q^q \\ & f & \mapsto & (f(0), f(1), \ldots, f(q-1)) \end{array}$$

O código de Reed-Solomon (de grau 1) é a imagem de L por ϕ. Denotaremos este código por RS.

É fácil ver que este código é MDS: cada polinômio não-nulo de L só tem um zero em F_q, e por isso $d = q-1$. Como $k = 2$ e $n = q$, temos a igualdade $k + d = n + 1$.

O grupo de simetrias pode ser calculado de modo análogo ao do código de Reed-Muller.

Teorema 19 *O grupo de simetrias de RS é isomorfo a $S_q^q \rtimes S_q$.*

Demonstração. Seguindo os mesmos passos da demonstração para o código de Reed-Muller, tome o grafo Γ com vértices em RS e arestas $(\phi f, \phi g)$ tais que $f-g$ é constante. Os automorfismos de Γ são as isometrias de RS. De fato, existem apenas dois pesos em RS, e basta usar o mesmo raciocínio anterior. Como antes, este grafo também é feito da união de grafos completos. Suas componentes são os conjuntos $K(ax) = \{\phi(ax+b); b \in F_q\}$, sendo portanto q componentes de q pontos cada. Por argumentos análogos aos do caso Reed-Muller, os automorfismos de Γ podem ser decompostos como produtos $\sigma\pi$, onde π é uma permutação de componentes, e $\sigma = (\sigma_0, \sigma_1, \ldots, \sigma_{q-1})$ é um automorfismo que fixa as componentes. Em termos dos pontos de RS, temos

$$\begin{array}{rcl} (\sigma_0, \sigma_1, \ldots, \sigma_{q-1})(\phi(ax+b)) & = & \phi(ax + \sigma_a(b)) \\ \pi(\phi(ax+b)) & = & \phi(\pi(a)x + b) \end{array}$$

Todas as permutações de componentes são possíveis, e cada componente é um grafo completo. Portanto, o grupo pode ser escrito como GH, onde G é isomorfo a S_q^q e H, ao grupo S_q. Pelas mesmas contas do caso anterior, obtemos que $Aut(\Gamma)$ é isomorfo a $S_q^q \rtimes S_q$. ■

[3]Todo código satisfaz a inequação $k + d \leq n + 1$ (para espaços de Hamming). Quando vale a igualdade, o código é chamado MDS (maximum distance separable).

Usando esta decomposição de $\mathbb{S}(RS)$ é fácil construir rotulamentos cíclicos. Tomamos novamente um q-ciclo π de S_q e um q-ciclo σ' de S_q, definimos $\sigma = (\sigma_1, \ldots, \sigma_{q^{m-1}}) \in S_q^q$ por

$$\sigma_i = \begin{cases} \sigma', \text{ se } i = 1 \\ id, \text{ caso contrário.} \end{cases}$$

e tomamos $\phi = \sigma\pi$. Esta simetria tem ordem q^2 e rotula o código. Concluindo,

Teorema 20 *O código de Reed-Solomon RS pode ser rotulado por um grupo cíclico de isometrias.*

Nós observamos que estes códigos também não são metricamente rígidos (isto foi mostrado em [40]).

4.3.3 Estimativas sobre a ordem de simetrias em $\left(\mathbb{Z}_p^{p^n}, d\right)$

Voltando aos códigos de Reed-Muller, uma coisa que chama a atenção é a taxa do código (a razão k/n). A taxa de $RM(1,m)_q$ é muito baixa , e uma questão que se coloca naturalmente é se existem rotulamentos cíclicos de códigos com taxas maiores. Nós podemos fornecer uma resposta parcial a esta pergunta estudando o grupo de simetrias de $\left(\mathbb{Z}_p^{p^n}, d\right)$. Para isto vamos precisar apenas de um pequeno resultado sobre ordens de elementos e de um subgrupo p-Sylow particular de $\mathbb{S}\left(\mathbb{Z}_p^{p^n}, d\right)$. Quanto a este último, utilizaremos a identificação $\mathbb{S}\left(\mathbb{Z}_p^{p^n}, d\right) \cong S_p^{p^n} \rtimes S_{p^n}$.

Lema 7 *[13] Seja G um grupo finito e N e H subgrupos de G, com N abeliano e normal em G.*

1. *Sejam $n \in N$ e $h \in H$. Então $|nh|$ divide $|n|\,|h|$.*
2. *Suponha que $N \cap H = \{id\}$, de modo que podemos formar o grupo $N \rtimes H$. Então a ordem de h divide a ordem de nh.*

Demonstração. A primeira afirmação segue da equação

$$(nh)^r = n(hnh^{-1})(h^2nh^{-2})\ldots(h^{r-1}nh^{r-1})h^r.$$

Se $|n| = r$ e $|h| = s$, então

$$(nh)^{rs} = \left[n(hnh^{-1})(h^2nh^{-2})\ldots(h^{s-1}nh^{s-1})\right]^r.$$

Como a aplicação $n \mapsto h^k n h^{-k}$ é um isomorfismo para cada k, $|n| = \left|h^k n h^{-k}\right|$. Como o grupo N é normal, a expressão à direita da igualdade só envolve elementos de N. Usando a comutatividade, obtemos

$$\begin{aligned} (nh)^{rs} &= \left[n(hnh^{-1})(h^2nh^{-2})\ldots(h^{s-1}nh^{s-1})\right]^r \\ &= n^r(hnh^{-1})^r(h^2nh^{-2})^r\ldots(h^{s-1}nh^{s-1})^r \\ &= id. \end{aligned}$$

Isto prova a primeira afirmação. Para a segunda, considere a projeção

$$\begin{array}{rccc} p: & N \rtimes H & \to & N \\ & nh & \mapsto & n \end{array}$$

que é um homomorfismo sobrejetor. Então, como $(n)^{|nh|} = p\left(nh^{|nh|}\right) = p\left(id\right) = id$, temos que $|h|$ divide $|nh|$. ■

Teorema 21 *Seja f uma isometria de $\left(\mathbb{Z}_p^{p^n}, d_h\right)$. Se a ordem de f é uma potência de p, então $|f| \leq p^{n+1}$.*

Demonstração. Seja f uma isometria que tem ordem p^k. Recordamos aqui alguns dos resultados dos teoremas de Sylow: se G é um grupo com ordem $p^s b$, sendo p e b coprimos, então existe um subgrupo de ordem p^s. Um subgrupo com esta ordem é chamado de p-Sylow. Todos os p-Sylows são conjugados em G, e se f é um elemento de ordem p^k, então f pertence a algum p-Sylow.

No nosso caso, temos

$$\left|S_p^{p^n} \wr S_{p^n}\right| = (p!)^{p^n}\left(p^n!\right) = p^{(n+(n-1)+\ldots+1)} p^{p^n} b = p^{p^n+\left((n^2+n)/2\right)} b,$$

e existe então um subgrupo H de $S_p^{p^n} \wr S_{p^n}$ de ordem $p^{p^n+\left((n^2+n)/2\right)}$ que contém f, pois $|f| = p^k$. Para estimar o máximo expoente k, vamos usar um subgrupo de $S_p^{p^n} \wr S_{p^n}$ que contém um outro p-Sylow conjugado a este.

Em $S_p^{p^n}$ temos o p-Sylow $\mathbb{Z}_p^{p^n}$ (o grupo de translações). Seja G um p-Sylow de S_{p^n}. O grupo gerado por G e $\mathbb{Z}_p^{p^n}$ é um produto semi-direto, $\mathbb{Z}_p^{p^n} \wr G$, porque $\mathbb{Z}_p^{p^n}$ é invariante sob a ação de S_{p^n} (por conjugação). Sua ordem é $p^{\left(n^2+n\right)/2} p^{p^n}$ e portanto este é um grupo de Sylow de $S_p^{p^n} \wr S_{p^n}$. O grupo H que contém f é conjugado a $\mathbb{Z}_p^{p^n} \wr G$, e podemos examinar as ordens de elementos neste grupo para concluir sobre a ordem de f. Para simplificar, tomaremos f no grupo $\mathbb{Z}_p^{p^n} \wr S_{p^n}$, que contém $\mathbb{Z}_p^{p^n} \wr G$. Veremos que a estimativa assim obtida é ótima.

Seja $f = g\pi$ um elemento de $\mathbb{Z}_p^{p^n} \wr S_{p^n}$, e suponha que $|f| = p^k$. Pelo Lema 7, p^k divide $|g|\,|\pi|$. Como a ordem de g é p ou 1, p^{k-1} divide a ordem de π. Logo, se $\pi = c_1 c_2 \ldots c_s$ é a decomposição de π em ciclos disjuntos, algum c_i tem comprimento p^{k-1} ou p^k. Como o comprimento máximo de um ciclo é a dimensão do espaço, p^n, temos que $p^{k-1} \leq p^n$, ou seja, $p^k \leq p^{n+1}$. Observamos que esta estimativa é ótima: o elemento $f = (1, 0, \ldots, 0)\,(12 \ldots p^n)$ tem ordem p^{n+1}. ■

Assim, se um código C em $\left(\mathbb{Z}_p^{p^n}, d_h\right)$ é parametrizado por um subgrupo cíclico de $\mathbb{S}\left(\mathbb{Z}_p^{p^n}, d_h\right)$ de ordem potência de p, este código tem no máximo p^{n+1} pontos. Esta estimativa indica que as parametrizações de códigos de Reed-Muller devem estar próximo do melhor possível em termos de número de pontos rotulados. No entanto, este resultado não leva em conta as simetrias de códigos que não se estendem ao espaço ambiente, e por isso pode haver algum código com uma simetria cíclica de ordem maior que a dada pelo último teorema. No entanto, ainda não

foi encontrado nenhum rotulamento cíclico que passe a barreira de p^{n+1}, e as simetrias não-extensíveis já aparecem de modo fundamental nos rotulamentos dos códigos de Reed-Muller binários, como veremos a seguir.

4.3.4 Rotulamentos do Reed-Muller binário de primeira ordem

Existe uma forma básica de estudar códigos binários como códigos esféricos que é a identificação entre espaços de Hamming e o conjunto de vértices de n-cubos em $\mathbb{R}^n$. Isto já foi utilizado neste trabalho na construção de exemplos de códigos G-lineares e propelineares (capítulo 3). Esta identificação é essencial nesta seção, e começamos por suas propriedades básicas.

Seja $\beta = \{e_1, \ldots, e_n\}$ uma base ortonormal de $\mathbb{R}^n$, e considere a aplicação

$$\begin{array}{rccc} \eta: & \mathbb{Z}_2^n & \longrightarrow & \mathbb{R}^n \\ & (a_1, \ldots, a_n) & \mapsto & \sum_{i=1}^n (-1)^{a_i} e_i \end{array}$$

Seja $C_n = [-1,1]^n = \{\sum_{i=1}^n a_i e_i | -1 \leq a_i \leq 1\}$ o hipercubo associado à base β, e seja $C(n)$ o conjunto de vértices deste hipercubo. Considere $C(n)$ como um espaço métrico, com função distância induzida pela métrica euclidiana. A aplicação η estabelece uma correspondência entre códigos esféricos contidos em $C(n)$ e códigos binários. Embora η não seja uma isometria, muitas propriedades geométricas são compartilhadas entre o código $\mathcal{C}$ e sua imagem $\eta(\mathcal{C})$. Em especial, seus grupos de simetrias são isomorfos - no sentido de [13], podemos dizer que eles possuem a mesma configuração métrica. Costuma-se usar a aplicação η no estudo de códigos de Kerdock e de funções curvadas (bent functions; ver p.ex. [27, 10]).

Proposição 2 *Seja $\beta = \{v_1, \ldots, v_n\}$ uma base ortonormal de $\mathbb{R}^n$, e seja $\eta : \mathbb{Z}_2^n \to \mathbb{R}^n$ a aplicação associada. Então*

(i)[27] Para u, v in $\mathbb{Z}_2^n$, $\langle \eta u, \eta v \rangle = n - 2d_h(u,v)$;

(ii) Para cada código $\mathcal{C}$ em $\mathbb{Z}_2^n$, η induz um isomorfismo de grupos entre $\mathbb{S}(\mathcal{C})$ and $\mathbb{S}(\eta(\mathcal{C}))$.

Demonstração.

(i) $\langle \eta u, \eta v \rangle = \sum_{i=1}^n (-1)^{u_i + v_i} = -w_h(u+v) + (n - (w_h(u+v)) = n - 2w_h(u+v) = n - 2d_h(u,v)$.

(ii) Segue diretamente de (i). Seja g um elemento de $\mathbb{S}(\eta(\mathcal{C}))$; então $\langle g\eta u, g\eta v \rangle = \langle \eta u, \eta v \rangle$ para todos u, v em $\mathcal{C}$. Seja g^η a função $g^\eta = \eta^{-1} g \eta : \mathcal{C} \to \mathcal{C}$. A aplicação $g \mapsto g^\eta$ é um homomorfismo, e, por (i),

$$\begin{array}{rcl} w_h(g^\eta u + g^\eta v) & = & 1/2(n - \langle \eta g^\eta u, \eta g^\eta v \rangle) \\ & = & 1/2(n - \langle g\eta u, g\eta v \rangle) \\ & = & 1/2(n - \langle \eta u, \eta v \rangle) \\ & = & w_h(u+v). \end{array}$$

■

No problema de extensão da $\mathbb{Z}_4$-linearidade, vários artigos trataram disto do ponto de vista de isometrias entre módulos e códigos. Como foi explicado no Capítulo 1 (lema 1), isto é equivalente a trabalhar com isometrias dentro do código. Nesta parte usaremos a aplicação η para descrever todos os rotulamentos cíclicos do código de Reed-Muller binário de primeira ordem - que correspondem aos obtidos anteriormente. Estes rotulamentos serão descritos via o grupo de simetrias do código esférico associado $\eta(RM(1,m))$. Este é um código biortogonal em $\mathbb{R}^{2^m}$, e seus rotulamentos cíclicos são facilmente descritos.

Definição 26 *Um código esférico C em $\mathbb{R}^n$ é dito biortogonal se é obtido do "referencial duplo" $B = \{\pm e_1, \ldots, \pm e_n\}$ por rotação e/ou semelhança.*

O fato que $\eta(RM(1,m))$ é biortogonal é conhecido na literatura mas, como não encontramos nenhuma referência com uma demonstração, incluimos uma na proposição a seguir.

Proposição 3 *Seja $\beta = \{v_1, \ldots, v_{2^m}\}$ uma base ortonormal de $\mathbb{R}^{2^m}$, e seja $\eta : \mathbb{Z}_2^{2^m} \to \mathbb{R}^{2^m}$ a aplicação associada.Então*

(i) O código de Reed-Muller $RM(1,m)$ é levado por η sobre um código biortogonal em $\mathbb{R}^{2^m}$.

(ii) Dada uma função afim f de $\mathbb{Z}_2^m$, seja $H(f) = \{f + h; h = \sum a_i x_i, a_i \in \mathbb{Z}_2\}$ (a classe lateral de $\mathcal{O}_m$ que contém f). Então cada ordenação de $H(f)$ induz um rotulamento cíclico de $RM(1,m)$.

Demonstração.

(i) Como já visto, o polinômio enumerador de $RM(1,m)$ é $t^{2^m} + (2^{m+1} - 2)t^{2^{m-1}} + 1$. Como o código é homogêneo (é linear), este é o perfil de distâncias para qualquer ponto. Em outras palavras, para qualquer g em $RM(1,m)$, existem $2^{m+1} - 2$ pontos h no código tais que $\langle \eta g, \eta h \rangle = 2^m - 2(2^{m-1}) = 0$, e também que existe um ponto h (que é o ponto $g + 1$) tal que $\langle \eta g, \eta h \rangle = 2^m - 2(2^m) = -2^m$. Portanto, $C = \eta(RM(1,m))$ é um código biortogonal com vetores de norma $N = 2^m$.

(ii) Primeiro descreveremos os grupos cíclicos que parametrizam o código biortogonal $C = \eta(RM(1,m))$. A cada base $\beta \subset C$ corresponde uma simetria T que rotula C; se $\beta = \{v_1, \ldots, v_{2^m}\}$, então T é a transformação linear definida por

$$Tv_i = \begin{cases} v_{i+1}, i = 1, \ldots, 2^m - 1 \\ -v_1, i = 2^m. \end{cases}$$

A ordem de T é 2^{m+1} e T percorre todo o código C. Por outro lado, dada $T \in \mathbb{S}(C)$ tal que o grupo $\langle T \rangle$ age livre e transitivamente em C, temos que a ordem de T é 2^{m+1} e que o conjunto $\beta(T, v) = \{v, Tv, \ldots, T^{2^m - 1}v\}$ tem que ser uma base de $\mathbb{R}^{2^m}$ para qualquer $v \in C$. Basta ver que se existe $0 < k < 2^m$ com $T^k v$ em $\langle \{v, Tv, \ldots, T^{k-1}v\} \rangle$, então $T^k v = T^j v$ para algum $j \neq k$, pois $T(C) = C$. Daí $T^{k-j}v = v$, e a ação de $\langle T \rangle$ não é livre, constradição.

Deste modo, temos uma correspondência entre bases contidas em C e grupos cíclicos que rotulam C. Por outro lado, seja $H(f) = \{f + h; h = \sum a_i x_i, a_i \in \mathbb{Z}_2\}$ a classe lateral de $\mathcal{O}_m$ em $RM(1,m)$ que contém f. Pela proposição 2, temos

$$\langle \eta f, \eta(f + h) \rangle = 2^m - 2w(h) = 2^m - 2\left(2^{m-1}\right) = 0.$$

Como $H(f)$ tem exatamente 2^m elementos, $\eta(H(f))$ é uma base de $\mathbb{R}^{2^m}$. A recíproca é válida pela mesma conta: qualquer base β é levada em um "hiperplano" $\mathcal{O}_m + f$. Isto estabelece uma bijeção entre as classes $\mathcal{O}_m + f$ e as bases contidas em C, a menos da ordem dos vetores de cada base. Como já tínhamos uma bijeção entre rotulamentos e bases, segue que existe uma bijeção entre ordenações de classes laterais $\mathcal{O}_m + f$ e rotulamentos. ■

Um último ponto a ser demonstrado é que estes rotulamentos de $RM(1,m)$ são feitos por simetrias que não podem ser estendidas ao espaço ambiente. A prova é feita por uma simples estimativa sobre a ordem de uma isometria. Para isso usamos a novamente a fatoração de uma simetria g como $\pi\tau_u$, onde π é uma permutação de coordenadas e agora τ_u é a translação por um vetor u.

Teorema 22 *Seja g uma simetria do código binário de Reed-Muller $RM(1,m)$. Se g define um rotulamento, então g não se estende a uma simetria própria de $(\mathbb{Z}_2^{2^m}, d_h)$.*

Demonstração. Seja $g \in \mathbb{S}(2^m) \ltimes \mathbb{Z}_2^{2^m}$, $g = (\pi, u)$, e suponha que $|g| = 2^k$ para algum k. Pela demonstração do Teorema 21, sabemos que $k \leq m+1$ e que se $|g| = 2^{m+1}$, então $|\pi| = 2^m$. Seja C um código binário contido no código $[2^m, 2^m - 1] = \{v \in \mathbb{Z}_2^{2^m}; \sum_{i=0}^{2^m} v_i = 0\}$, e g uma simetria deste código do tipo $g = (\pi, u)$ (ou seja, extensível). Então a ordem de g é menor do que ou igual a 2^m. Para ver isso, suponha que $|\pi| = 2^m$, ou seja, que π é um 2^m-ciclo. Em particular, cada sequência $\{s, \pi(s), \pi^2(s), \ldots, \pi^{2^m-1}(s)\}$ é apenas um rearranjo da sequência $\{1, 2, 3 \ldots, 2^m\}$. Como $g^r = (\pi^r, \sum_{i=0}^{r-1} \pi^{-i} u \pi^i)$,

$$\begin{aligned} \sum_{i=0}^{2^m} \pi^{-i} u \pi^i &= \left(\sum_{i=0}^{2^m} u_{\pi^{-i}(1)}, \ldots, \sum_{i=0}^{2^m} u_{\pi^{-i}(n)} \right) \\ &= \left(\sum_{i=0}^{2^m} u_i, \ldots, \sum_{i=0}^{2^m} u_i \right) \\ &= 0, \end{aligned}$$

portanto $g^{2^m} = id$. A outra possibilidade é que $|\pi| < 2^m$, mas aí temos $|g| \leq |\pi|\,|u| < 2^{m+1}$.

Segue que não existe simetria de $(\mathbb{Z}_2^{2^m}, d_h)$ que preserve $RM(1,m)$ e tenha ordem 2^{m+1}. Todos os rotulamentos cíclicos são feito por isometrias não-extensíveis, e o código não é metricamente rígido.

4.4 Perspectivas Futuras

Os resultados obtidos neste trabalho sugerem o caminho para abordar alguns problemas correlatos e também sugerem novas questões envolvendo simetrias de códigos. Nós destacamos as seguintes questões:

Simetrias extensíveis dos códigos de Reed-Muller $GRM(1,m)_q$

Neste trabalho nós descrevemos as simetrias do código de Reed-Muller. No entanto, com exceção do caso binário, não conhecemos ainda o grupo das simetrias extensíveis, isto é, o grupo $\mathbb{S}\left(GRM(1,m)_q, F_q^{q^m}\right)$ das simetrias que são induzidas do espaço ambiente (embora o grupo de automorfismos já seja conhecido [4]). Determinar este grupo é uma questão importante para uma melhor caracterização geométrica do código, e também é um caminho para descobrir a natureza dos rotulamentos cíclicos dos códigos de Reed-Muller.

Estimativas sobre a menor taxa possível para rotulamentos cíclicos

Um caminho alternativo ao de estudar códigos em R-módulos a partir de isometrias entre estes módulos e códigos de Hamming é partir diretamente do módulo. Isto é, primeiramente se estuda um peso (ou classe de pesos) sobre um módulo M, esboça-se uma teoria de códigos para este caso, e depois busca-se uma isometria entre M e um código de Hamming [16, 23]. A questão sobre qual a taxa mais baixa para um rotulamento por $\mathbb{Z}_m$ existir vem destes trabalhos.

No caso binário existe o caminho de considerar o problema associado na esfera, como feito aqui várias vezes. Este pode ser um modo de resolver o problema, pois todos os grupos de simetria de códigos em $\mathbb{Z}_2^n$ se encontram no grupo ortogonal real $O(n)$, o que nos dá um ponto de partida. No presente trabalho a questão foi resolvida para códigos cujas simetrias são todas induzidas. Para seguir as mesmas idéias da demonstração, o que buscamos é um subgrupo discreto H de $O(n)$ que contenha todos os grupos de simetria de uma classe razoável de códigos. As contas sobre os rotulamentos possíveis viriam de estimativas sobre a ordem de elementos de H.

Códigos perfeitos corretores de 1 erro em espaços de Lee

Neste trabalho nós estudamos os códigos perfeitos lineares em dimensão 2. Em [20] são descritos códigos corretores de 1 erro em dimensão n. O resultado é:

Teorema 23 *[20] Dado n inteiro positivo, sejam $q = 2n+1$ e C o núcleo de $\lambda : \mathbb{Z}_q^n \to \mathbb{Z}_q$, $\lambda(x) = \sum_{i=1}^n ix_i$. Então C é um código perfeito de distância 3 no espaço de Lee sobre $\mathbb{Z}_q^n$.*

Na verdade, pode-se mostrar facilmente que todos os códigos lineares perfeitos (corretores de 1 erro) são descritos como núcleos de funcionais do tipo

$$(-1)^{a_1} x_{\pi^{-1}(1)} + (-1)^{a_2} 2x_{\pi^{-1}(2)} + \ldots + (-1)^{a_n} nx_{\pi^{-1}(n)},$$

onde π é uma permutação e $a_i = 0, 1$. Isto sugere que haja uma ação do grupo $\mathbb{Z}_2^n \rtimes S_n$ no conjunto destes códigos. Isto é verdade, e todos estes códigos são equivalentes, exatamente como no caso bidimensional. Várias questões ainda restam, entre as quais destacamos a descrição dos grupos de automorfismos e a existência ou não de códigos perfeitos não-lineares além dos transladados dos lineares. A resposta a ambas as questões passa pelo cálculo do grupo de automorfismos do código $\sum_{i=1}^n ix_i = 0$. Para isso pode ser vantajoso utilizar as conexões entre códigos e reticulados, e fazer este cálculo via o grupo de automorfismos do reticulado associado, $L_n = \{(a_1, \ldots, a_n) \in \mathbb{Z}^n; \sum_{i=1}^n ia_i = 0 \bmod (2n+1)\}$.

Referências Bibliográficas

[1] Agustini, Edson, Constelações de Sinais em Espaços Hiperbólicos. Tese de Doutorado, IMECC, Unicamp, 2002.

[2] Araújo, Martinho da Costa, Caracterizações algébrica e geométrica dos códigos propelineares. Tese de Doutorado, FEE, Unicamp, 2000.

[3] Araújo, M.C.; Palazzo Jr., R.; Muniz, M.; Costa, S., Caracterização Geométrica dos Códigos Propelineares e a Não Existência de Códigos Propelineares m-ários, $m \geq 3$., in: atas (CD-ROM) do congresso "XVIII Simpósio Brasileiro de Telecomunicações" , 03-06 de setembro de 2000, Gramado, RS.

[4] Berger, Thierry; Charpin, Pascale, The automorphism group of generalized Reed-Muller codes. Discrete Math. 117 (1993), no. 1-3, 1–17.

[5] Berlekamp, Elwyn R., Algebraic coding theory. McGraw-Hill Book Co., New York-Toronto, Ont.-London 1968

[6] Borges, Joaquim; Rifà, Josep, A characterization of 1-perfect additive codes. IEEE Trans. Inform. Theory 45 (1999), no. 5, 1688–1697.

[7] Calderbank, A. R.; Sloane, N. J. A., Modular and p-adic cyclic codes. Des. Codes Cryptogr. 6 (1995), no. 1, 21–35.

[8] Calderbank, A. R.; Li, Wen-Ching Winnie; Poonen, Bjorn, A 2-adic approach to the analysis of cyclic codes. IEEE Trans. Inform. Theory 43 (1997), no. 3, 977–986.

[9] Carlet, Claude, $\mathbb{Z}_{2^k}$-linear codes. IEEE Trans. Inform. Theory 44 (1998), no. 4, 1543–1547.

[10] Carlet, Claude, On Kerdock Codes. Contemporary Mathematics, vol.225, 1999, 155-163.

[11] Conway, J. H.; Sloane, N. J. A., Sphere packings, lattices and groups. Grundlehren der Mathematischen Wissenschaften, 290. Springer-Verlag, New York, 1999.

[12] Costa, Sueli I.R.; Agustini, E.; Muniz, M.; Palazzo, R., Graphs, Tesselations and Perfect Codes on Flat Tori. Preprint.

[13] Costa, Sueli Rodrigues; Gerônimo, João Roberto; Palazzo, Reginaldo, Jr.; Interlando, J. Carmelo; Alves,Marcelo Muniz Silva, The symmetry group of $\mathbb{Z}_q^n$ in the Lee space and the $\mathbb{Z}_{q^n}$-linear codes. Applied algebra, algebraic algorithms and error-correcting codes (Toulouse, 1997), 66–77, Lecture Notes in Comput. Sci., 1255, Springer, Berlin, 1997.

[14] Costa, Sueli; Agustini, Edson; Muniz, Marcelo; Palazzo Jr., Reginaldo, Slepian-Type Codes on Flat Tori. Preprint.

[15] Constantinescu, Ioana; Heise, Werner. On the concept of code-isomorphy. J. Geom. 57 (1996), no. 1-2, 63–69.

[16] Constantinescu, Ioana; Heise, Werner, A metric for codes over residue class rings of integers. Problems Inform. Transmission 33 (1997), no. 3, 208–213.

[17] Duursma, Iwan M.; Greferath, Marcus; Litsyn, Simon N.; Schmidt, Stefan E. A $\mathbb{Z}_8$-linear lift of the binary Golay code and a nonlinear binary $(96, 2^{37}, 24)$-code. IEEE Trans. Inform. Theory 47 (2001), no. 4, 1596–1598.

[18] Marcelo Firer, Grupos Fuchsianos. Notas de aula.

[19] Geronimo, João R., Extensão da $\mathbb{Z}_4$-linearidade via grupos de simetrias. Tese de Doutorado, FEEC,Unicamp, 1997.

[20] Golomb, Solomon, W. Tiling with polyominoes. J. Combinatorial Theory 1 1966 280–296.

[21] Greferath, Markus; Schmidt, Stefan E., Gray isometries for finite chain rings and a nonlinear ternary $(36, 3^{12}, 15)$ code. IEEE Trans.Inform. Theory 45 (1999), no. 7, 2522–2524.

[22] Hammons, A. Roger, Jr.; Kumar, P. Vijay; Calderbank, A. R.; Sloane, N. J. A.; Solé, Patrick, The $\mathbb{Z}_4$-linearity of Kerdock, Preparata, Goethals, and related codes. IEEE Trans. Inform. Theory 40 (1994), no. 2, 301–319.

[23] Honold, T.; Landjev, I., Linearly representable codes over chain rings. Abh. Math. Sem. Univ. Hamburg 69 (1999), 187–203.

[24] Huber, Klaus, Codes over Gaussian integers. IEEE Trans. Inform. Theory 40 (1994), no. 1, 207–216.

[25] Huber, Klaus, Codes over Eisenstein-Jacobi integers. Finite fields: theory, applications, and algorithms (Las Vegas, NV, 1993), 165–179, Contemp. Math., 168, Amer. Math. Soc., Providence, RI, 1994.

[26] McDonald, Bernard R., Finite rings with identity. Pure and Applied Mathematics, Vol. 28. Marcel Dekker, Inc., New York, 1974.

[27] MacWilliams, F. J.; Sloane, N. J. A., The theory of error-correcting codes. North-Holland Mathematical Library, Vol. 16. North-Holland Publishing Co., Amsterdam-New York-Oxford, 1977.

[28] Muniz, M. e Costa,S., Labelings of Lee and Hamming Spaces. Preprint. Artigo a ser publicado no periódico "Discrete Mathematics".

[29] Muniz, M. e Costa,S., $\mathbb{Z}_4$-linearity cannot be strictly extended to Hamming spaces, Relatório de Pesquisa RP32/01, IMECC, Unicamp.

[30] Alves, M.M.S., Códigos Geometricamente Uniformes em Espaços de Lee. Dissertação de mestrado, IMECC, Unicamp, 1998.

[31] Alves, M.M.S.; Gerônimo, J.R.; Palazzo Jr., R.; Costa, S.I.R.; Interlando, J.C.; Araújo, M.C., Relating propelinear and binary G-linear codes, Discrete Mathematics 243 (2002), no.1-3, 187-194.

[32] Nechaev, A. A., Kerdock's code in cyclic form. Discrete Math. Appl. 1 (1991), no. 4, 365–384

[33] Nechaev, A.; Kuzmin, A., Linearly Presentable Codes. Proc. 1996 IEEE Int. Symp. Inf. Theory Appl., Victoria B.C., Canadá, 1996, 31-34.

[34] Pires da Nóbrega Neto, Trajano; Interlando, J. Carmelo; Favareto, Osvaldo Milaré; Elia, Michele; Palazzo, Reginaldo, Jr., Lattice constellations and codes from quadratic number fields. IEEE Trans. Inform. Theory 47 (2001), no. 4, 1514–1527.

[35] Racsmány, A. O. H., Perfect single-Lee-error-correcting code. Stud. Sci. Math. Hungar. 9 (1974), 73–75 (1975).

[36] Racsmány, A., Correction to my paper: "Perfect single Lee-error-correcting code" Studia Sci. Math. Hungar. 23 (1988), no. 1-2, 295–296.

[37] J. Rifà, J. M. Bassart and L. Huguet, On Completely Regular Propelinear Codes, in Proc. 6th. Int. Conf., AAECC-6, Lecture Notes in Computer Science, n.357, Springer-Verlag, New York, 1989, pp. 341-355.

[38] J. Rifà and J. Pujol, Translation-invariant propelinear codes. IEEE Trans. on Inform. Theory, vol. IT-43, n.2, March 1997, pp. 590-598.

[39] Salagean-Mandache, Ana, On the isometries between $\mathbb{Z}_{p^k}$ and $\mathbb{Z}_p^k$. IEEE Trans. Inform. Theory 45 (1999), no. 6, 2146–2148.

[40] Solov'eva, Faina I.; Avgustinovich, Sergei V.; Honold, Thomas; Heise, Werner, On the extendability of code isometries. J. Geom. 61 (1998), no. 1-2, 3–16.

[41] Tsfasman, M. A.; Vladut, S. G., Algebraic-geometric codes Mathematics and its Applications (Soviet Series), 58. Kluwer Academic Publishers Group, Dordrecht, 1991.

[42] Wielandt, Helmut, Finite permutation groups. Translated from the German by R. Bercov Academic Press, New York-London 1964